Journal of Business & Technology Law

Volume 18 | Issue 2 Article 6

Cyberwarfare & Cyber Insurance: Exploring When a Cyberattack Can Negate a Cyber Insurance Claim

Joseph Michael Rovetto Jr.

Cyberwarfare & Cyber Insurance: Exploring When a Cyberattack Can Negate a Cyber Insurance Claim

JOSEPH MICHAEL ROVETTO JR.*

INTRODUCTION

If you had never heard of Mondelēz International, Merck Shipping, and did not know how a Russian malware attack could cripple the entire globe, you would probably be like most people. Two lawsuits, one originating in Cook County, Illinois,[1] and the other in Union County, New Jersey,[2] highlight what happens when a nation state creates and deploys malware designed to indiscriminately destroy everything it touches. Combined, these cases have the potential to upend the underdeveloped cyber-insurance market and force both businesses and insurance companies to rethink how they approach cybersecurity and cyber insurance policies.[3] This paper will explore three topics: (1) the history of the law of war and how international norms define and interpret a "hostile action", (2) how past insurance cases have interpreted the terms of art "hostile action" and "warlike operation"; and (3) analyze whether NotPetya qualified as a hostile action or warlike operation under both international and U.S. insurance law.

Ultimately, this paper will show that (1) under international law, NotPetya constituted an illegal armed attack against civilians,[4] (2) that because attacks against civilians are not actions that belligerents have recourse to during war, Merck and Mondelez were not engaged in actions that qualify as a hostile or

*© J.D. Candidate, 2023, University of Maryland Francis King Carey School of Law. The author thanks his fellow editors at the Journal of Business & Technology Law for all of their support in finalizing this article. The author also thanks Professor Markus Rauschecker for his teaching, guidance, and mentorship as the author wrote this comment and progressed throughout law school. Next, the author thanks his friends, especially Kaska Watson, Victoria Roman, Matt Dumont, Robert Velazquez, Betsy Schick, Caitlin Gugliotta, and Randall Ainsworth who, regardless of how long they have known him, have become a second family to him. Finally, the author dedicates this comment to his late father, Joe Rovetto, his mother, Ann Rovetto, for surviving a battle with breast cancer during the author's final year of law school, his brother, Michael Brantley for his support and friendship throughout their lives, his fiancée, Carley Becker, for her love and encouragement, and his beloved fur baby Zoey, who has been the best companion one could hope for.

1. Mondelēz Int'l, I v. Zurich Am. Ins., 2018-L-011008 (Ill. Cir. Ct. filed Oct. 8, 2019).
2. Merck & Co., Inc. vs. Ace Am. Ins., No. L-002682-18 (N.J. Super. Ct. Law Div. Aug. 02, 2018).
3. Cybersecurity & Infrastructure Sec. Agency, Assessment of Cyber Insurance Market, (study finds the cyber insurance market underdeveloped…Council of Insurance Agents & Brokers and PwC characterize the cyber insurance market as "soft" [emphasis added]).
4. *See infra* Section IV.B

warlike action under U.S. insurance law,[5] (3) that the losses suffered by Merck and Co. and Mondelēz International were because of their proximity to the general internet, not the hostilities in Ukraine, and (4) that the internet as whole cannot, and must not, be considered a theater of war.[6]

I. HISTORY OF NOTPETYA

In June 2017, an alleged ransomware attack spread across the globe like wildfire. Affecting everything from ports, to hospitals, to shipping companies, NotPetya left very few industries alone.[7] Even federal institutions, were victims to this virulent ransomware attack.[8] One of the more high-profile victims of the attack, A.P. Møller-Maersk, saw their entire shipping operation, which is the largest in the world, abruptly halted because of the malicious code.[9] While NotPetya appeared to be a run-of-the-mill ransomware attack, there was supposedly a way to "pay a ransom" to unlock a victimized computer system, this turned out to only be a ruse.[10] Attempting to pay the ransom achieved nothing, and it was later determined that there was no way to unlock the encrypted files in most systems. While companies such as Mondelēz and Merck were not the primary targets of the malware, they were swept up in the attack as collateral damage.[11]

The real target of NotPetya was the Ukrainian government and its various business and financial sectors, and the perpetrators of the attack were not cyber criminals interested in making a quick dollar.[12] Instead, the source of the malware came from within Russia's General Staff Main Intelligence Directorate ("GRU").[13] The group, informally known around the world as the "Sandworm Team," had previously conducted attacks against the Ukrainian government as part of Russia's ongoing conflict in the region.[14] The attack caused devasting losses across Ukraine;

5. *See infra* Section IV.C.

6. *See infra* Section IV.C.2.

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

8. *Id.*

9. *Id.*

10. *Id.*

11. *Id.*

12. *Id.*

13. David Voreacos et al., *Merck Cyberattack's $1.3 Billion Question: Was It an Act of War?*, BLOOMBERG NEWS (Dec. 3, 2019, 12:01 AM), https://news.bloomberglaw.com/privacy-and-data-security/merck-cyberattacks-1-3-billion-question-was-it-an-act-of-war?context=search&index=6; *see also* Press Release, Dep't. Just., Six Russian GRU Officers Charged, (Oct. 19, 2020) (on file with Dep't. Just.).

14. Chris Strohm & Alyza Sebenius, *U.S. Charges 6 Russian Agents for Hacking That Cost Billions*, BLOOMBERG LAW (Oct. 20, 2020, 8:52 AM), https://www.bloomberglaw.com/bloomberglawnews/privacy-and-

it shutdown entire financial institutions, disrupted hospitals, and even shut down the nuclear radiation monitors at the defunct Chernobyl nuclear plant.[15] Because the malware encrypted entire computer systems, whole networks had to be replaced within the country.[16]

In the aftermath of the attack, businesses across the world suffered devastating losses. One of the plaintiffs, Merck & Co., suffered over $1 billion in damages.[17] Other companies, such as A.P. Møller-Maersk, saw its entire fleet stranded at sea or stuck in various ports of call around the world.[18] Shortly after the NotPetya attack, companies affected by the malware filed insurance claims to recover from the nearly $10 billion in damages NotPetya caused.[19] Of all the companies who suffered losses, two stand out from the pack, at least in the United States. Merck & Co. and another company, Mondelēz International, have become infamously connected with NotPetya.[20] This is not because of the financial harm suffered by the companies, but because the companies' respective insurance companies denied Merck's and Mondelēz's cyber insurance claims based on a rarely used industry policy, the war clause exclusion.[21] The next section will briefly introduce the war clause exclusion and how it is used within the insurance industry.

A. Understanding Insurance Risk and the War Exclusion

Because war brings such high risk of destruction and mayhem, general liability and property insurance contracts have generally excluded the dangers and risks associated with war.[22] However, despite provisions in insurance contracts that attempt to limit an insurance company's obligation,[23] courts have routinely found that unless a claimed loss was *directly related* to a war or "hostile action,"

data-security/XDG0S7UC000000?bna_news_filter=privacy-and-data-security#jcite; *see generally Sandworm Team*, (last accessed Oct. 18, 2021) https://attack.mitre.org/groups/G0034.

15. Voreacos et al., *supra* note 13.

16. *Id.*

17. Dep't Just., *supra* note 13; Voreacos et al., *supra* note 13.

18. Voreacos et al., *supra* note 13.

19. *Id.*

20. *See id.*; *see also* Adam Satariano & Nicole Perlroth, *Big Companies Thought Insurance Covered a Cyberattack. They May Be Wrong*, NEW YORK TIMES (April 15, 2019), https://www.nytimes.com/2019/04/15/technology/cyberinsurance-notpetya-attack.html.

21. *See supra* Voreacos et al., *supra* note [13]13.

22. *See generally* Queen Ins. Co. v. Globe & Rutgers Fire Ins. Co., 263 U.S. 487, 44 S. Ct. 175 (1924).

23. Jeffrey W. Stempel, *The Insurance Aftermath of September 11: Myriad Claims, Multiple Lines, Arguments Over Occurrence Counting, War Risk Exclusions, the Future of Terrorism Coverage, and New Issues of Government Role*, 37 TORT & INS. L.J. 817, 848 (2002) ("language in Queen Insurance contract excluded 'all consequences . . ., of hostilities or warlike operations.'").

insurance companies are obligated to cover the loss.[24] Thus, courts have differentiated between a "cause in fact and a sufficiently proximate cause (in time or dominance) [that] trigger[s] or preclude[s] insurance coverage."[25]

Unfortunately, at the time of this writing,[26] the specific arguments the insurance companies are making in the *Mondelēz* and *Merck* cases are not publicly available. While the author attempted to get specific arguments from summary judgement motions in both cases, the respective courts in those cases have placed protective orders around most documents. Certain documents that were obtained, however, give a glimpse into the specific arguments the insurance companies are making.[27] In *Mondelēz*, Zurich Insurance denied coverage based on the policy's war clause exclusion, which specifically states:

"This Policy excludes loss or damage directly or indirectly caused by or resulting from any of the following . . . a) hostile or warlike action in time of peace or war . . .."[28]

Based on this filing, this paper will explore whether ancillary victims such as Mondelēz International and Merck Shipping should be treated the same as direct targets of a hostile nation for purposes of an insurance contract.

II. LAW OF WAR: DEFINITION OF ARMED ATTACK

Before delving into the current controversies surrounding the *Mondelēz* and *Merck* cases, an understanding of some of the bedrock principles and arguments being made in the cases is necessary.

The *Mondelēz* and *Merck* cases highlight a question that has been discussed since the Stuxnet virus was first released against Iran's nuclear centrifuges: do the traditional norms of warfare apply to the digital realm of cyberspace? The short answer is yes. The general consensus in the international community is that cyber warfare must follow the norms of traditional warfare.[29] The more nuanced

24. *Id.*; *compare* Int'l Dairy Eng'g Co. v. Am. Home Assurance Co., 474 F.2d 1242 (9th Cir. 1973) (finding that the dropping of a flare was a warlike operation and was the proximate and most direct cause of the loss); *with* Pan Am. World Airways, Inc. v. Aetna Cas. & Sur. Co., 505 F.2d 989 (2d Cir. 1974) (rejecting arguments that a political terrorist groups actions in an airplane hijacking equated to a warlike action, thus establishing the proximate cause of the loss as a terrorist hijacking).

25. Stempel, *supra* note 23.

26. December 2021.

27. The vast majority of documents that were obtained for this article come from the *Mondelēz* case. However, according to various blogs and reports on the cases, the insurance company in *Merck* is relying on the same war clause exclusion. Because most of the documents in *Merck* are under seal and unavailable to the public, this case will be treated as making the same argument for the purposes of this paper.

28. Motion for Defendants at Exhibit D, Mondelēz Int'l, I v. Zurich Am. Ins., 2018-L-011008 (Ill. Cir. Ct. filed on Oct. 8, 2019).

29. For existing cybersecurity norms, *see* Richard A. Clarke, *Good Harbor Securing Cyberspace Through International Norms*, Good Harbor Security Risk Management, LLC (2013),

answer, however, is that it is not always easy to draw parallels between traditional warfare and cyberwarfare, and thus, determining whether a cyber action is an "armed attack"[30] within the laws of war is not always clear cut. There are commentators who believe that the release of NotPetya did not rise to the level of an "armed attack" under the traditional *casus belli* (cause for war) because it had no real-world destruction or death, and thus should not be considered a "hostile action"[31] by a foreign adversary for insurance purposes.[32] While the end conclusion of these arguments are correct, that NotPetya should not be considered a "hostile action" for purposes of the *Merck* and *Mondelēz* cases, these commentators are mistaken that NotPetya was not an armed attack under international law and have only applied a narrow lens to what happened in Ukraine.[33] The following subsection will explore the terms "armed attack" as understood by the United Nations ("UN") General Assembly and how international law applies to cyberspace and cyber operations. It will introduce several key concepts that will apply in analyzing whether the release of the NotPetya malware was a hostile action or warlike operation under U.S. insurance law.[34]

A. The United Nations

In the wake of World War II, the world was in shambles and countries were scrambling to pick up the pieces.[35] After months of negotiations, nearly fifty countries signed onto the newly created United Nations Charter, including Chapter VII Article 51, Action with respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression.[36] Article 51 states, "Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an *armed attack* occurs against a Member of United Nations . . .."[37] What is an armed attack though? If data cannot carry a gun, directly kill someone, or drop a bomb, can it

https://carnegieendowment.org/files/Good-Harbor_Securing-Cyberspace-Through-International-Norms_2013.pdf; *see also* N. ATL. TREATY ORG. COOP. CYBER DEF. CTR. EXCELLENCE, Tallinn Manual 2.0 (Michael N. Schmitt et al. eds., 2nd ed. 2017) [hereinafter Tallinn Manual 2.0].

30. Tallinn Manual 2.0, *supra* note 29 at 340 (differentiating between a use of force and an armed attack and defining an armed attack as an act of aggression by one Nation State against another).

31. *See infra* Section III.A.

32. Matthew P. McCabe, *NotPetya Was Not Cyber "War,"* MARSH MCLENNAN (Aug. 2018), https://www.marshmclennan.com/insights/publications/2018/aug/notpetya-was-not-cyber-war.html.

33. *See supra* Section I; *see also infra* Section V.B.

34. *See infra* Section 0. It is important to note here that international law is not the same as U.S. law. The laws of war, absent binding international agreements to which the United States is a signatory, do not apply in U.S. courts and can only be used as a persuasive influence in determining whether certain criteria are met.

35. *History of the United Nations*, U.N., (last visited Dec. 12, 2021) https://www.un.org/en/about-us/history-of-the-un.

36. U.N. Charter art. 51 (1945).

37. *Id.* (emphasis added).

still constitute an armed attack against a country? To help answer this question, we turn to Article 2(4) of the UN Charter which will help define the term "armed attack" and whether a cyber attack can satisfy *jus ad bellum*.[38]

Article 2(4) states, "All Members shall refrain from the threat or use of force against the territorial integrity or political independence of any state . . .."[39] There are three primary ways to interpret the prohibition on force.[40] In relation to a cyber attack, one such way is directly relating a cyber attack to a kinetic response;[41] another is determining whether a cyber attack was coercive in nature, similar to that of applying economic or political pressure;[42] and, finally, another is whether a cyber attack has violated the sovereign dominion of a state.[43] If one adheres to the first interpretation, then a cyber attack that has no kinetic repercussions in the physical world, then very few cyber attacks would ever satisfy the doctrine of *jus ad bellum*. Though we have increasingly seen cyber attacks cause physical destruction,[44] and even death,[45] these attacks have been relatively rare.[46] If one applies the broader coercive or interference interpretation to a cyber action, that greatly broadens the scope of what can be considered a hostile cyber attack by a foreign nation. This latter view is similar to how one leading authority, the Tallinn Manual, interprets and analyzes cyber operations.[47]

B. The Tallinn Manual 2.0

The Tallinn Manual was drafted by a group of international experts with one goal in mind: apply standing international principles on the law of armed conflict to cyberspace. Many of the principles developed throughout the last century of warfare can be found within its script, and it lays a legal foundation for how to view cyber operations and digital warfare on the international stage.

38. *See* U.N. Charter art. 2(4) (1945) (*Jus ad bellum* stands for the legal framework in which countries can justify going to war).

39. *Id.*

40. *See* Matthew C. Waxman, *Cyber-Attacks and Use of Force: Back to the Future of Article 2(4)*, 36 YALE L.J. 421, 431-32 (2011).

41. *Id.*

42. *Id.*

43. *Id.*

44. David P. Fidler, *Just & Unjust War, Uses of Force & Coercion: An Ethical Inquiry with Cyber Illustrations*, 145 DAEDALUS 37 (2016).

45. AP News, *Suit Blames Baby's Death on Cyberattack at Alabama Hospital*, AP (Oct. 1, 2021), https://apnews.com/article/technology-business-health-alabama-lawsuits-68c78e9d6af359842c0e9645b4577b50.

46. *See* Joseph Marks, *Ransomware Attack Might Have Caused Another Death*, WASH. POST (Oct. 1, 2021, 7:07 AM), https://www.washingtonpost.com/politics/2021/10/01/ransomware-attack-might-have-caused-another-death.

47. *Infra* Section II.B.

Generally, nation states must refrain from deliberately targeting civilian populations,[48] and according to the International Court of Justice, this rule is "intransgressible."[49] Under international law, the use of propaganda, including cyber propaganda that targets civilians, is not prohibited.[50] However, if a cyber operation rises to the level of an "attack," then that operation is prohibited under the principle of distinction[51] and customary international law.[52] The international group of experts who wrote the Tallinn Manual defined a cyber attack as "a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects."[53] The group of experts also uniformly agreed the existence of physical destruction (i.e. fire or a giant hole in the ground from kinetic strike) was not necessary for a cyber operation to qualify as a cyber attack.[54] Further, cyber attacks must be "against [an] adversary" in order to qualify as a lawful cyber attack, limiting the target to legitimate military targets.[55]

Physical damage is not required in order to be labeled an attack.[56] The group of experts likened cyber attacks to biological warfare: there might not be an explosion that releases kinetic energy, however, that does not stop people from dying.[57] Thus, the "crux of the notion lies in the effects. . . [T]he consequences of an operation, not its nature, are what generally determine the scope of the term 'attack'."[58] The group of experts discussed two scenarios where a cyber operation could meet the criteria of being an armed attack.[59] First, if a cyber operation caused terror amongst a civilian population, the operation would qualify as an attack, since "terror is a psychological condition resulting in mental suffering."[60] Second, if a cyber operation results in the permanent loss of an entire control system or of vital components in a control system, the operation qualifies as an attack, as it has met a sufficient threshold of harm.[61]

48. Tallinn Manual 2.0, *supra* note 29 at Rule 94.

49. *Id.*, at Rule 93.

50. *Id.* at 421.

51. Protocol Additional to the Geneva Convention relating to the Protection of Victims of International Armed Conflicts (Protocol I) art. 48, Jun. 8, 1977, 1125 U.N.T.S. 3.

52. *Id.*; *see also* Tallinn Manual 2.0 *supra* note 29 at 423, (citing various State military manuals such as the DoD Manual, UK Manual, etc.).

53. *Id.* at Rule 92.

54. *Id.*

55. *Id.*

56. *Id.*

57. *Id.*

58. *Id.*

59. *Id.*

60. *Id*.

61. *Id.*

III. DEFINING TERMS OF ART UNDER U.S. LAW

Though the issue of cyber warfare might be relatively new to the insurance industry, business loss during times of war is not, and the insurance industry has developed unique terms to determine when and how to deploy certain phrases such as "war", "warlike", and "hostile action."[62] U.S. courts must turn to past insurance cases to find binding precedent.[63] While U.S. courts can turn to international law for help in guiding a decision,[64] it is not automatically binding precedent. Consequently, international norms remain only a helpful tool for courts to interpret how a cyberattack should be viewed. The following subsections introduce various terms of art and how U.S. courts have interpreted and applied them.

A. Hostile Action - Past Insurance Cases

1. TRT/FTC Communications v. Ins. Co.

TRT/FTC Communications[65] centered around the U.S. invasion of Panama. During the 1989 invasion, eight people dressed as civilians and carrying military style weapons looted the plaintiffs and made off with a variety of expensive equipment.[66] The defendant denied the plaintiffs' insurance claim based on the war exclusion clause in their insurance contract.[67] The court found that because the Panamanian government declared war on the U.S., the war was the proximate cause of the looting and that the looting was therefore enabled by active military hostilities, regardless of whether the individual looters were part of the military or not.[68] The looters were therefore "qualifying belligerents," and the plaintiffs were ineligible to recover due to the war exclusion in its insurance policy.[69]

2. International Dairy Engineering Co. v American Home Assurance Co.

International Dairy stems from a warehouse fire in South Vietnam during the Vietnam War.[70] The plaintiff was the victim of a fire caused by a parachute flare

62. Universal Cable Prods., LLC v. Atl. Specialty Ins. Co., 929 F.3d 1143, 1160 (9th Cir. 2019).

63. *Supra* text accompanying note 34.

64. *See* Pan Am. World Airways, Inc. v. Aetna Cas. & Sur. Co., 505 F.2d 989, 1022 n12 (2d Cir. 1974) ("Of course international law definition of war does not necessarily govern the insurance meaning of the term . . . but it provides a starting place for our inquiry.").

65. TRT/FTC Commc'ns v. Ins. Co., 847 F. Supp. 28 (D. Del. 1993), *aff'd*, 9 F.3d 1541 (3rd Cir. 1993).

66. *Id.*

67. *Id.* at 29.

68. *Id.* at 30.

69. *Id.*

70. Int'l Dairy Eng'g Co. v. Am. Home Assurance Co., 474 F.2d 1242 (9th Cir. 1973).

that landed in the middle of the plaintiff's box stock.[71] The plaintiff's insurance policy specifically stated that fire was not excluded "unless caused directly . . . by a hostile act . . . or against a belligerent power."[72] The plaintiff's insurance company denied coverage for the fire based on the war clause exclusion, and the plaintiff subsequently sued.[73] On appeal, the plaintiff argued that the parachute was not dropped during the course of normal warfare operations, but was instead negligently dropped by a pilot during a routine flight.[74] The appellate court reviewed evidence stating that the dropping of the parachute flare was in connection with "military operations against [the] Viet Cong."[75] Further, the court affirmed the lower trial courts' finding that the proximate and direct causes, of the fire were the hostile actions of a known belligerent.[76] The appellate court concluded these causes were sufficient to establish that the dropping of the parachute flare was a "hostile act" in operations against the Viet Cong. Thus, because a hostile action was the "proximate, direct cause of the loss," the insurance company was not responsible for coverage.[77]

B. War or Warlike Action – Past Insurance Cases

Although there is some overlap in the definitions of the terms "warlike action" and "hostile action," they are distinct terms that have different meanings.[78] Because one of the potential arguments in the *Mondelēz* and *Merck* cases is that the NotPetya attack was part of an ongoing warlike operation,[79] reviewing the case law will be useful in determining whether or not the NotPetya attack was in fact a warlike operation.[80]

71. *Id.* at 1243.

72. *Id.*

73. *Id.*

74. *Id.* at 1242-43.

75. *Id.*

76. *Belligerent*, Black's Law Dictionary (11th ed. 2019) ("Belligerent: One engaged in a war or other armed conflict.").

77. *Int'l Dairy*, 474 F.2d at 1243.

78. *Compare Hostile Act*, BLACK'S LAW DICTIONARY (11th ed. 2019) ("Hostile Act: an event that may be considered an adequate cause of war"), *with* Steven Plitt, et al., COUCH ON INSURANCE § 152:4 (3d ed. 2017) ("Warlike operations are normally [defined] as being part of an armed conflict between combatants . . .").

79. Voreacos, *supra* note 13.

80. *See Cyberforce*, BLACK'S LAW DICTIONARY (11th ed. 2019) ("Cyberforce: the use of computers to carry out warlike conduct.").

1. Pan American World Airways v. Aetna Casualty Surety Co.

Pan Am.[81] is one of the earliest cases that delves into the nuances of whether an action is hostile or warlike by a foreign government.[82] In 1970, Pan American Flight 083 was hijacked by members of the Popular Front for the Liberation of Palestine ("P.F.L.P"), a terrorist organization that was dedicated to "softening" Israel's stance on Palestine.[83] The Ninth Circuit ultimately sided with Pan American World Airways ("Pan Am") by deciding that the damages to Pan Am were not conducted by a government entity during the course of war or warlike operations.[84]

The court distinguished between an action taken by a non-governmental linked group attacking non-combatants and a sovereign government attacking another sovereign government. The court determined that attacks on "civilian citizens of non-belligerent powers and their property at places far removed from the locale or the subject of any warfare 'would not qualify as "warlike operations."'"[85] In its analysis, the Ninth Circuit turned to international law to determine the definition of war.[86] The court found that traditionally "war" was defined as "contention between two or more States through their armed forces."[87] This created a link between international law and U.S. courts in defining the term when it stated that "English and American cases dealing with the insurance meaning of 'war' have defined it in accordance with the ancient international law definition."[88] The Ninth Circuit concluded that to engage in "war" or "warlike operations," the entities involved must hold at least "significant attributes of sovereignty"[89] and that the actor must be at least a "de facto government."[90]

Next, the Ninth Circuit analyzed whether the P.F.L.P. was a "de facto government."[91] The court determined that the P.F.L.P was a political force that often "acted independently from other Palestinian entities,"[92] such as the Palestine Liberation Organization ("P.L.O.").[93] The court rejected the argument

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

82. *Id.*; *see also* Scott J. Shackelford, Comment, *Wargames: Analyzing The Act Of War Exclusion In Insurance Coverage And Its Implications For Cybersecurity Policy*, 23 Yale J.L. & Tech. 362 (2021).

83. *1970 Hijackings,* PBS (last accessed Nov. 1, 2021), https://www.pbs.org/wgbh/americanexperience/features/hijacked-1970-hijackings/.

84. *Pan Am.*, 505 F.2d at 1015-17.

85. *Id.* at 1016.

86. *Id.* at 1012.

87. *Id.*

88. *Id.*

89. *Id.* at 1012.

90. *Id.* at 1009.

91. *Id.* at 1009-12.

92. *Id.* at 1006.

93. The P.L.O. was the precursor to the Palestinian Authority, who today is the ruling body in Palestinian. Both a political group and a terrorist organization, the P.L.O. was an early Palestinian political organization

that because King Hussein negotiated for the release of hostages, the P.F.L.P. should be treated as a government.[94] The court also rejected the argument that the P.F.L.P. possessed significant attributes of sovereignty because the land was essentially a wasteland.[95] The court determined that the P.F.L.P was not a "de facto government" when the plane was hijacked,[96] that Pan Am Flight 083 was not hijacked during a warlike act,[97] and the plane involved was not engaged in any conceivable warlike operation that would justify exclusion under the insurance policy.[98]

2. Universal Cable Prods., LLC v. Atlantic Specialty Ins. Co.

In a more recent case,[99] Universal Cable filed suit against its insurer after a TV show the company was filming was forced to withdraw from Jerusalem.[100] The production team was forced to leave the city after Hamas launched rockets from Gaza into Israel.[101] The insurance company denied coverage based on several provisions in the war clause exclusion of the insurance contract;[102] however, the Ninth Circuit ultimately rejected the insurance company's arguments, reversed the district court's findings for summary judgment, and remanded the case for further proceedings.[103]

The Ninth Circuit reiterated its previous ruling from *Pan Am* that "war" and "warlike action" (operations) require hostilities between de jure or de facto sovereigns.[104] Relying on the treatise Appleman on Insurance, the court defined "war" as a "'course of hostility' between 'states or state-like entities.'"[105] Regarding the "warlike actions" provision of the insurance contract in question, the court noted that the phrase "warlike actions" was derived from the phrase "warlike operations."[106] The court stated that to be a "warlike operation" the action must be "of such a general kind or character as belligerents have recourse

and still exists today. *See Palestine Liberation Organization (P.L.O.)* (May 3, 2022), https://www.adl.org/resources/glossary-terms/palestine-liberation-organization-plo*; see also Palestinian Authority* (last accessed Dec. 12, 2021), https://www.adl.org/resources/glossary-terms/palestinian-authority.

94. *Pan Am.*, 505 F.2d at 101.
95. *Id.* at 1011-12.
96. *Id.* at 1009.
97. *Id.* at 1014.
98. *Id.* at 1017.
99. *See generally* Universal Cable Prods. LLC vs. Atl. Specialty Ins. Co., 929 F.3d 1143 (9th Cir. 2019).
100. *Id.* at 1147.
101. *Id.*
102. *Id.*
103. *Id.* at 1162-63.
104. *Id.* at 1147.
105. *Id.* at 1154.
106. *Id.* at 1159.

to in war"[107] and that such operations must be carried out by the military forces of a sovereign or quasi-sovereign government.[108]

In layman's terms, a hostile act that would qualify would be an attack against a military target, such as a supply depot.[109] Further, that attack must be carried out by military forces that represent at least a quasi-government that has some semblance of legitimacy.[110] An example would be if the recently exiled Afghanistan President[111] raised arms against the Taliban and began attacking military targets to regain control of the country. Assuming the attacks were against legitimate military targets, the attacks would qualify under the "warlike operations" definition, as the ex-President could be considered a quasi-sovereign (or usurped military power)[112] and the Taliban can be considered the new government of Afghanistan.

3. Airlift International, Inc. v. United States

Airlift International, Inc. stems from the loss of a plane due to a midair collision.[113] Specifically, the plaintiff lost an aircraft after a midair collision with a U.S. Airforce reconnaissance plane.[114] The plaintiff's plane was under contract with the U.S. government, and was transporting "general cargo" under a military contract to an airbase in Vietnam.[115] The loss occurred when a U.S. Air Force aircraft collided with the civilian plane.[116] During the subsequent trial, the district court analyzed whether either plane was involved in a warlike operation and, if so, whether the operation was the proximate cause of the loss. The court hinged its decision on the fact that a proximate cause inquiry must establish that the loss was the consequence of a warlike operation, not whether the loss happened in the course of a warlike operation.[117]

The court determined that particular risks were associated with certain trades.[118] Thus, aviation companies had to accept certain risks in order to fly planes, the same as shipping companies accepted certain risks in order to sail and

107. *Id.*

108. *Id.*

109. For a more detailed discussion, *see infra* Section IV.B.

110. *See* Universal Cable Prods. LLC vs. Atl. Specialty Ins. Co., 929 F.3d 1143, 1160 (9th Cir. 2019).

111. *Ashraf Ghani: Afghanistan's exiled president lands in UAE* (Aug. 18, 2021), https://www.bbc.com/news/world-asia-58260902.

112. *See* Pan Am. World Airways, Inc. v. Aetna Cas. & Sur. Co., 505 F.2d 989, 1009-10 (2d Cir. 1974).

113. Airlift Int'l, Inc. v. United States, 335 F. Supp. 442 (S.D. Fla. 1971).

114. *Id.* at 445-46.

115. *Id.* at 447.

116. *Id.*

117. *Id.* at 448.

118. *Id.* at 446.

transport goods.[119] The district court found in favor of the plaintiffs first by determining that the transportation of cargo, even military cargo, did not satisfy the requirements for participating in a warlike operation.[120] Citing the U.S. Supreme Court in *Standard Oil Company of New Jersey v. United States*,[121] the court rested its decision on the Court's finding that "not only must [a] vessel's mission be one of war, but the warlike character of its operation must be the dominant and effective cause of the resulting catastrophe."[122]

The court also declared that even if the plane had been participating in a warlike operation, the plaintiffs could still recover as the proximate cause of the plane's loss was from the general risk that comes with flying planes, not any particular warlike operation.[123] The court noted that "[an] inquiry should be whether the collision was a *consequence* of a warlike operation, not did it happen in the course of a warlike operation."[124] Thus, even if the loss of a plane happened during a warlike operation, if the operation itself was not the direct and proximate cause of the loss, then an insured is not barred from recovery.

C. Summary

Past case law has given courts a roadmap for determining when an action can be considered hostile or warlike. As exemplified above, courts use a proximate cause analysis to determine the cause of a loss.[125] As introduced in Section IV, insurance policies use terms of art such as "hostile action" and "warlike operations" that have special meaning in U.S. courts and in the insurance industry. Section IV also showed how courts have interpreted and applied those terms. To be considered either a "hostile action" or "warlike operation," two factors must be present: (1) there must be at least two entities that have at least de-facto or quasi-sovereign attributions, and (2) those entities must be engaged in some type of conflict that is traditional with warfare.[126]

When applying these factors to the NotPetya attack, we see that the use of NotPetya has different meanings depending on what stage it is on,[127] however, the next section will show that NotPetya clearly does not meet the definition of

119. *Id.*
120. *Id.* at 447.
121. 340 U.S. 54, 58 (1950).
122. *Airlift Int'l*, 335 F. Supp. at 447.
123. *Id.* at 447.
124. *Id.* at 448.
125. *See supra* notes 24, 68-69, 77 and accompanying text.
126. *Supra* notes 85-90 and accompanying text.
127. I.e. international law vs. U.S. courts.

"hostile act" or "warlike operations" as U.S. courts understand and apply those terms.[128]

V. ANALYSIS

The previous sections outlined the rules, case law, and requirements for determining whether an action can be excluded under a war exclusion clause in an insurance contract.[129] This section will apply the international norms and the rules of past case law to argue that (1) the NotPetya attack was a hostile act or warlike act within the meaning of the war exclusion clause, (2) the direct victims of the attack would rightly be denied coverage, but (3) due to policy reasons, ancillary victims such as Mondelēz and Merck should not be barred from recovering under their respective insurance contracts.

A. Recap

In review, Mondelēz International and Merck and Co. were both victims of the NotPetya malware that swept across the globe in 2018.[130] The alleged perpetrator behind the malicious code was publicly attributed by various sources to the Russian military, specifically a specialized division within the GRU.[131] Both companies filed claims under their respective insurance policies to recover from the damage, and both were denied coverage under the war exclusion clause that is common to most commercial insurance policies.[132] While the insurance companies' exact arguments are unavailable,[133] reasonable inferences regarding the insurance companies purported arguments can be drawn from numerous commentators[134] and some of the sparse documents that are available to the public.[135]

B. Was NotPetya Cyberwarfare - Internationally?

The Russian military deployed the NotPetya cyber attack in an attempt to disrupt the Ukrainian government by targeting its business and financial sectors. The

128. *See infra* Section IV.C.1.

129. *See supra* Sections II-III.

130. *See supra* Section I.

131. Strohm & Sebenius, *supra* note 14.

132. Voreacos et al., *supra* note 13.

133. At least as of the time of publication.

134. Jon Bateman, *War, Terrorism, and Catastrophe in Cyber Insurance: Understanding and Reforming Exclusions*, Carnegie Endowment for Int'l Peace (Oct. 05, 2020), https://carnegieendowment.org/2020/10/05/war-terrorism-and-catastrophe-in-cyber-insurance-understanding-and-reforming-exclusions-pub-82819; *see also* McCabe, *supra* note 32.

135. Motion, *supra* note 28.

attack was part of the ongoing conflict the Russian government has had with Ukraine since 2014,[136] and the specific team responsible, codenamed Sandworm,[137] is notorious for launching cyberattacks against various Ukrainian interests during the conflict.[138] In the aftermath of the NotPetya incident, some commentators argued that the malware attack was more akin to a propaganda tool that was only meant to cause disruption.[139] These commentators are wrong.

International law makes it clear that civilians cannot be targets of an offensive operation, and this principle applies to cyber warfare.[140] Under international law, cyber operations are required to follow the same laws and norms as real-world kinetic operations.[141] In fact, under the principle of distinction, when nation states deploy a weapon system, they must ensure that the weapon is able to distinguish between civilian and military targets.[142] Failure to do so can result in determinations that the attack was illegal and/or a war crime.[143] Additionally, as discussed in Section III.B., cyber operations do not have to cause physical destruction to constitute a cyber attack.[144]

The initial threat vector of the NotPetya malware was a tax accounting system called M.E.Doc that was widely used in Ukraine.[145] The malware was inserted into the program via a backdoor and then distributed to victim computers across Ukraine, and from there, the world.[146] Commentators that argue against labeling NotPetya a cyberattack[147] contend that because the majority of damage was done outside of Ukraine, because no deaths occurred, and because there was no physical damage, the malware does not qualify as a cyber attack.[148] These arguments ignore, dismiss, or minimize what actually happened inside Ukraine and only view the malware attack in light of a single action, instead of viewing the

136. Voreacos et al., *supra* note 13.

137. Strohm & Sebenius, *supra* note 14.

138. John Hulquist, *Sandworm Team and the Ukrainian Power Authority Attacks*, MANDIANT (Aug. 23, 2022), https://www.mandiant.com/resources/ukraine-and-sandworm-team.

139. McCabe, *supra* note 32; see also Danny Palmer, *NotPetya Malware Attack: Chaos but not Cyber Warfare* (Aug. 16, 2018), https://www.zdnet.com/article/notpetya-malware-attack-chaos-but-not-cyber-warfare.

140. Tallinn Manual 2.0, *supra* notes 48-49 and accompanying text.

141. *Id.*

142. *Id.* at Rule 93; *see also* Geneva Add. Protocols, *supra* note 51.

143. *Definition of War Crimes*, Int'l. Comm. Of the Red Cross (last accessed Apr. 13, 2023), https://ihl-databases.icrc.org/en/customary-ihl/v1/rule156.

144. *See supra* Section III.B.

145. John Fruhlinger, *Petya Ransomware and NotPetya Malware: What You Need to Know Now* (Oct. 17, 2017, 2:59 AM PDT) https://www.csoonline.com/article/3233210/petya-ransomware-and-notpetya-malware-what-you-need-to-know-now.html.

146. *Id.*

147. McCabe, *supra* note 32.

148. *Id.*

malware attack in light of the years-long undeclared war between Russia and Ukraine.

The malware shut down ten percent of all computers in Ukraine and paralyzed networks across a wide swath of industries, including critical infrastructure such as hospitals, airports, and power companies.[149] Further, the malware crippled nearly every Ukrainian government agency network[150] and shut down the radiation monitors at Chernobyl.[151] NotPetya was clearly designed as an indiscriminate cyberweapon,[152] as the malware (1) targeted civilians,[153] (2) shut down hospitals, ATMs, card payment systems,[154] and other key critical infrastructure systems that were guaranteed to cause panic in the civilian populace, and (3) was clearly designed to destroy whatever computer system it came in contact with, causing critical damage to tens of thousands of non-military computer systems.[155] Given these facts, it is clear that the introduction of NotPetya into the Ukrainian cyber infrastructure constituted an illegal attack under international law, and would thus qualify as an "armed attack" under the laws of war.

C. Analyzing the Mondelēz and Merck Cases under U.S. Law

NotPetya was, and should be considered, an illegal use of force under international law.[156] As discussed,[157] international definitions of terms do not have binding precedent under U.S. law.[158] International law can be persuasive, however, and can be used as a guide for determining if certain legal precedents

149. Satariano & Perlroth, *supra* note 20.

150. The Ukrainian minister of Infrastructure Volodymr Omelyan described the government as "dead." *Id.*

151. *Id.*

152. Tallinn Manual *supra* note 29 at 452 (cyber weapon defined as "cyber means of warfare that are used, designed, or intended to be used to cause injury to, or death of, persons or damage to, or destruction of, objects, that is, that result in the consequences required for qualification of a cyber operation as an attack [under Rule 92]").

153. *Id.* at Rule 93 n.1012. Targeting civilians clearly violates the principle of distinction, which, at its most basic level, states that Nation States should only target legitimate military targets. Regardless of whether the entry point of the malware could be considered a legitimate target, the virality of the malware clearly shows it was not designed to differentiate between military and civilian targets. Because it was reasonably foreseeable that the malware would spread in the manner that it did, it clearly violated nearly all international norms regarding the treatment of civilians.

154. Satariano & Perlroth, *supra* note 20.

155. Rae Ritchie, *Maersk: Springing Back From a Catastrophic Cyber-Attack*, I-CIO (Aug. 2019), https://www.i-cio.com/management/insight/item/maersk-springing-back-from-a-catastrophic-cyber-attack (noting that Maersk Shipping alone had to replace over 49,000 computers and 3,500 servers).

156. *Compare supra* notes 39-47 and accompanying text, *with* 139-155 and accompanying text.

157. *Supra* text accompanying note 34.

158. Pan Am. World Airways, Inc. v. Aetna Cas. & Sur. Co., 505 F.2d 989, (2d Cir. 1974), n12 ("Of course international law definition of war does not necessarily govern the insurance meaning of the term . . . but it provides a starting place for our inquiry.").

are met.[159] For the courts in the *Mondelēz* and *Merck* cases, resources such as the Tallinn Manual can be used to determine if the NotPetya incident is a hostile action "of such a general kind or character as belligerents have recourse to in war."[160]

This guidance is necessary, as analyzing and applying prior case law in the Mondelēz and Merck cases is difficult. On one hand, some case law gives credence to the suggestion that the NotPetya attack qualifies as either a "hostile act" or "warlike operation."[161] As shown in *TRT/FTC* and *International Dairy*, a civilian does not have to participate in the warlike operation to be denied coverage under a war exclusion policy.[162] The courts in those respective cases hinged their decisions on the fact that the warlike operation was the proximate cause of the loss. However, the respective courts in *Mondelēz* and *Merck* should not find this persuasive for two reasons: (1) the release of an indiscriminate malware such as NotPetya does not meet the standard of "actions taken during the course of war" and, hence, there was no warlike operation; and (2) as a matter of public policy, the internet as a whole cannot be considered a theater of operation for nation states conducting cyberattacks. Therefore, since Mondelēz and Merck were not participating in any warlike operation, they should not be subject to their insurance policies' war exclusion clause.[163]

1. A Cyber Weapon that Indiscriminately Targets Civilians is Illegal, and the Use of Such a Weapon is Not Consistent With Activities That "Belligerents Have Recourse to in War"

One of the key elements when applying a war exclusion clause is whether the action in question could be considered "of such a kind as belligerents have recourse to in war."[164] The court in *Pan Am* affirmatively ruled that the kidnapping of non-combatant civilians, far removed from a field of battle, did not qualify.[165] The release of NotPetya into the Ukrainain cyber infrastructure is similar to *Pan Am* in that the plaintiffs in the current cases were not involved in any military operation with Ukraine or Russia.[166] The *Pan Am* court listed several examples, such as transporting logistical supplies, that would qualify a civilian as being

159. *Id.*

160. Universal Cable Prods. LLC vs. Atl. Specialty Ins. Co., 929 F.3d 1143, 1159 (9th Cir. 2019).

161. *See supra* Section III.A.1 (reporting that an insured civilian victim was denied coverage due to ongoing hostilities between Panama and the United States).

162. *Id.; see also supra* Section III.A.2.

163. *See supra* Sections III.B.1-2.

164. *See supra* notes 107-112 and accompanying text.

165. Pan Am. World Airways, Inc. v. Aetna Cas. & Sur. Co., 505 F.2d 989, 1009, 1014, 1017 (2d Cir. 1974).

166. *Compare id.* at 998 (affirming lower court ruling that the kidnapping of civilians is not action comparable to warlike operations); *with* Voreacos, et al., *supra* note 13.

involved in a warlike operation.[167] No evidence has come to light that they were involved in any meaningful, or even remote, logistical transport of military goods to Ukraine or engaging in any other activity that would be considered a warlike operation. Thus, they were remote civilian victims, and could not be considered belligerents actively participating in war operations.

This finding is supported by other cases such as *Airlift International*.[168] In *Airlift International*, the court determined that the appropriate inquiry to determine whether the loss of a plane was the result of warlike operations was "whether the [loss] was a consequence of a warlike operation, not did it happen in the course of a warlike operation."[169] Based on the known information regarding Mondelēz's and Merck's insurance claims at the time of this paper's writing, the losses from both companies' appear to be losses that occurred in the course of the war between Ukraine and Russia, but not as a result of them. Thus, the proximate cause of the losses suffered by both Mondelēz and Merck stem not from the company's active participation or close proximity to a theater of operations, but from the general risk that is associated with being connected to the internet. Discussion as to whether the internet should or should not be considered a theater of war for the purposes of insurance is discussed in the following subsection.

2. The Internet Cannot be Considered a Theater of Operations for Nation States and, As a Matter of Public Policy, Victims Who Are Not Actively Participating in a Theater of War Should be Allowed to Collect Under Their Cyber Insurance Policies

Pan Am set forth one of the foundational rules that is critical to the present *Mondelēz* and *Merck* cases. As discussed in Section IV.B.1., to be considered either a hostile act or an action undertaken during a warlike operation, the action cannot be undertaken far removed from the theater of operations.[170] This requirement creates a temporal nexus that must be present in order to show that the conduct at issue is in the course of warlike operations.[171] Various courts seem to have supported this view as well.[172] In the context of a cyber attack, it is conceivable that a victim could be caught in the crosshairs of a cyber operation. The *Merck* and

167. *Pan Am.*, 505 F.2d at 1017.

168. *See* discussion *supra* Section III.B.3.

169. Airlift Int'l, Inc. v. United States, 335 F. Supp. 442, 448 (S.D. Fla. 1971).

170. *Pan Am.*, 505 F.2d at 1015-16.

171. *See id.*

172. *Compare id.*, *with* TRT/FTC Commc'ns v. Inc. Co., 847 F. Supp. 28 (D. Del. 1993), *aff'd*, 9 F.3d 1541 (3rd Cir. 1993), *and* Int'l Dairy Eng'g Co. v. Am. Home Assurance Co., 474 F.2d 1242 (9th Cir. 1973).

Mondelēz cases provide perfect examples of that reality.[173] NotPetya was deployed via a third-party system, M.E.Doc.[174] If M.E.Doc was to file a claim with its insurer, assuming U.S. jurisdiction and laws govern, then the insurance company would be within its right to deny the claim based on a war exclusion clause.[175] However, should the insurance companies in *Mondelēz* and *Merck* succeed in their argument, the entire internet would become a theater of operation.[176] It is imperative that this does not happen.

From a public policy standpoint, classifying the entire Internet as a legitimate theater of operations is untenable. In 2023, there are more devices capable of connecting to the Internet ("Internet of Things," or "IoT") than there are people in the world.[177] Each and every one of those devices is a potential threat vector for nation states seeking to execute cyber operations, and state-sponsored cyber activities has increased dramatically in recent years.[178] More nation states are relying on the cyber realm for offensive and espionage activities, with one report indicating a 100% rise in "significant" nation state incidents between 2017 and 2020.[179] These incidents range from espionage, to offensive cyber operations, to outright theft.[180] Because of the increased nation state activity, classifying the Internet as a theater of operations would place companies seeking cyber insurance at a significant disadvantage due to a reduced pool of available carriers.[181] Furthermore, the scarcity of carriers offering war insurance would result in dramatically higher prices.

173. *See generally* Mondelēz Int'l, I v. Zurich Am. Ins., 2018-L-011008 (Ill. Cir. Ct. filed Oct. 8, 2019), Merck & Co., Inc. vs. Ace Am. Ins., No. L-002682-18 (N.J. Super. Ct. Law Div. Aug. 02, 2018).

174. *See supra* note 140.

175. *Compare* discussion *supra* Section III, *with supra* note 145.

176. *See infra* note 177 and accompanying text (the logical conclusion of so many connected devices is that the entire internet would be considered a theater of operations as any device connected to the web is a potential threat vector).

177. *IoT Connections to Reach 83 Billion by 2024*, JUNIPER RESEARCH (Mar. 31, 2020), https://www.juniperresearch.com/press/iot-connections-to-reach-83-bn-by-2024.

178. Dr. Michael McGuire, Nation States, Cyberconflict and the Web of Profit (2021); *see also* Microsoft Digital Defense Report 2022, MICROSOFT (2022), https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bUvv?culture=en-us&country=us, *and* Kaspersky, *Cyberthreat Real-Time Map* (last accessed Apr. 14, 2023) https://cybermap.kaspersky.com/ (visual representation of actual cyber attacks or potential cyber attacks happening in real time).

179. McGuire, *supra* note 178; *see also* Microsoft, *supra* note 178.

180. *Id.*

181. *Compare Political Risk Insurance*, NATIONAL ASSOCIATION OF INSURANCE COMMISSIONERS (Oct. 20, 2022), https://content.naic.org/cipr-topics/political-risk-insurance (There is little direct information on how many insurance carriers offer war insurance. However, inferences can be drawn based on the number of carriers who offer Political Risk Insurance, which can include war. As of the NAIC's most recent report only 60 carriers offered Political Risk Insurance), *with* Memorandum from NAIC Staff on the Cyber Insurance Market (Oct. 18, 2022), https://content.naic.org/sites/default/files/cmte-c-cyber-supplement-report-2022-for-data-year-

Though it might seem unfair to force insurance companies to shoulder the burden of potential cyber attacks, they are not without recourse. Insurance companies can take the same data that is available to corporations seeking to purchase cyber insurance and raise premiums commensurate with the risk associated with the insurance.[182] Allowing the market to determine what level of risk should be associated with this rise in nation state activity is far preferable from a policy standpoint than allowing courts to determine that the Internet is a full-blown theater of war.[183] Though the absurdity doctrine is more often seen in statutory interpretation,[184] the courts in *Mondelēz* and *Merck* may still borrow from its principle and find that the ruling in favor of the insurance companies would have dire consequences for nearly every cyber insurance policy in existence today and put every public website, network, and IoT device squarely in a field of battle.

Had Mondelēz or Merck had their IT infrastructure located in Ukraine, or linked in any meaningful way to the Russian/Ukraine conflict, then arguably the insurance companies could make plausible arguments for denying coverage. Assuming those facts, the companies would fall more in line with past cases such as *International Dairy* and *TRT/FTC*. Both of those plaintiffs were located in a theater of war and suffered losses directly related to belligerents who were pursuing operations consistent with international law. However, neither Mondelēz nor Merck were functioning in the area of operations when NotPetya was released into the wild, nor were they actively supporting the Ukrainian government in any warlike capacity. Since merely being connected to the Internet is a general risk, like that of sailing a ship or flying a plane,[185] neither Mondelēz nor Merck should be penalized for falling victim to harms outside their control, which is one of the primary reasons that organizations purchase insurance in the first place. The mere fact that NotPetya was released by a nation state conducting hostile activities is not in and of itself sufficient to attribute the proximate cause of the companies' losses to a warlike operation.

2021.pdf (hereinafter NAIC Memo) (report prepared with data from 152 insurer groups representing 570 individual insurance companies).

182. Data suggests carriers are already participating in this manner, *see* NAIC Memo, *supra* note 181 (cyber insurance premiums increased 74% between 2020 and 2021).

183. *See supra* notes 177-181 and accompanying text.

184. Michael D. Cicchini, *The New Absurdity Doctrine*, 125 Penn St. L. Rev. 353, 356 (2021) ("The absurdity doctrine 'authorizes a judge to ignore a statute's plain words in order to avoid the outcome those words would require in a particular situation.'").

185. *See supra* Section III.B.3.

V. FOLLOW-UP PROCEEDINGS: A WIN FOR COMMON SENSE

The court in *Merck* issued a summary judgment ruling that the insurance carrier is not allowed to proceed with its claim that the act of war clause precluded paying for Merck damages.[186] While the court in *Merck* relied on several of the same cases as this article,[187] the lens and view from which the court rendered its judgment was vastly different. For this reason, an in-depth analysis of the court's reasoning is uncalled for and will be left for future publications and scholars. Regardless, the *Merck* court reached the correct conclusion by ruling against Ace American Insurance and finding that without further clarification at the time of entering the insurance contract, cyber warfare could have reasonably been expected to be separate from the general war exclusion clause.[188]

CONCLUSION

The *Mondelēz* and *Merck* cases present a novel issue to an old problem for the insurance industry: how to balance the risk of a loss. Insurance companies do not want to bear the brunt of the loss in cyber attack cases, and given the staggering amounts at stake, that is understandable. However, given the information available so far, the insurance companies in the *Mondelēz* and *Merck* cases should not be allowed to succeed on the merits of their arguments. Neither Mondelēz nor Merck were actively involved in an active warzone. Their IT infrastructure was only infected by the NotPetya malware because it was connected to the Internet, a risk all IoT devices face. Further, the development and use of NotPetya was in and of itself a violation of international law, and not conduct that ordinary combatants would have in the recourse of war. This is because the malware was designed to infect both civilian and military computer networks alike and was designed to cause chaos and fear in Ukrainian civilians. These characteristics disqualify the malware as a legitimate cyberweapon and make it an illegal use of force by the Russian government. For the reasons stated herein, the courts in *Mondelēz* and *Merck* should find in favor of the plaintiffs.

186. Order for Summary Judgement at 11, Merck & Co., Inc. vs. Ace Am. Ins., No. L-002682-18 (N.J. Super. Ct. Law Div. Aug. 02, 2018).

187. *Id.* at 9-10.

188. *Id.* at 11.