

MEALEY'S<sup>®</sup>

# Emerging Insurance Disputes

## Cyber War Exclusions

By  
*Peter A. Halprin*

*Haynes Boone  
New York, NY*

and

*Brittany Parks*

*Haynes Boone  
San Francisco and Orange County, CA*

A commentary article  
reprinted from the  
August 1, 2024 issue of  
Mealey's: Emerging Insurance  
Disputes



LexisNexis<sup>®</sup>



## Cyber War Exclusions

By  
**Peter A. Halprin**  
and  
**Brittany Parks**

*[Editor's Note: Peter A. Halprin is a partner in the Insurance Recovery Practice Group in Haynes Boone's New York office. Brittany Parks is an associate in the Insurance Recovery Practice Group in Haynes Boone's San Francisco and Orange County offices. Any commentary or opinions do not reflect the opinions of Haynes Boone or LexisNexis® Mealey Publications™. Copyright © 2024 by Peter A. Halprin and Brittany Parks. Responses are welcome.]*

In this day and age, one of the greatest risks that a company can face is that of a cyberattack. These attacks can come in many forms such as malware or ransomware, infecting the victim's computers to gain access to sensitive data and completely halt operations, and the losses stemming from such attacks can be devastating. For example, in 2017, the NotPetya malware resulted in more than \$10 billion in damages globally.<sup>1</sup>

Companies, however, can take some comfort in the fact that there are commercial insurance policies which provide coverage for such incidents. The issue, however, becomes more complicated insofar as insurers have sought to exclude such coverage, where state actors are involved, on the grounds that such actions are excluded acts of war, no different than what they have sought to traditionally exclude via so-called war exclusions in property insurance policies.

These issues were recently addressed by New Jersey courts which rejected insurer attempts to exclude the coverage for the NotPetya malware, on the grounds that the attacks did not fall within an exclusion for "war" or "warlike" action, allowing the policyholder to recover hundreds of millions of dollars.

As cyberattacks have increased, and perhaps in response to this decision, insurance companies have begun to incorporate new cyber exclusions in their policies.

This article will explore the history of traditional war exclusions, how courts have applied those exclusions in the context of cyberattacks, the recent introduction of war exclusions in the insurance market, and what comes next.

### **I. History of the War Exclusion as Applied to Traditional Warfare**

Because losses arising from war can be unpredictable and catastrophic, war-based exclusions have been incorporated into standard-form policies for centuries.<sup>2</sup> Beginning in the eighteenth century, insurers in the London-based Lloyd's market introduced an exclusion for "war risks" in marine policies in response to increasing war-related risks in the shipping trade.<sup>3</sup> War exclusions then began appearing across the United States since at least the Civil War, and saw an increase in use during the twentieth century as two world wars ensued.<sup>4</sup> Experts agree that the phrase "hostile or warlike action," or similar variants, have appeared in war exclusions since the 1950s.<sup>5</sup>

Iterations of the war exclusion have sought to preclude coverage not only for "war" but also for "warlike action" or "insurrection." While many versions of the war exclusion exist in the market, more recent war exclusions have precluded coverage for:

"Bodily injury" or "property damage", [sic] however caused, arising, directly or indirectly, out of:

- (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, usurped power, or action taken by governmental authority in hindering or defending against any of these.

Given the proliferation of war exclusions over the past century, many courts have had the opportunity to interpret these exclusions and the contours of what is excluded thereby.<sup>6</sup>

The Ninth Circuit Court of Appeals in *Universal Cable Prods., LLC v. Atlantic Specialty Ins. Co.* analyzed the first two prongs of the war exclusion for “war” and “warlike action.”<sup>7</sup> There, a television production company sought insurance coverage for losses associated with moving the production of one of its television series out of Jerusalem after Hamas fired rockets from Gaza into Israel. The insurer denied coverage, arguing that the war exclusion applied because Hamas’ actions constituted acts of “war” or “warlike action.” While the district court granted summary judgment to the insurer, the Ninth Circuit reversed, finding that neither prong of the exclusion applied. The Ninth Circuit reasoned that the terms “war” and “warlike action” had special meaning in the insurance context. Specifically, “war” requires “the existence of hostilities between de jure or de facto governments.”<sup>8</sup> And, “warlike action” requires (1) “operations of such a general kind or character as belligerents have recourse to in war,” and (2) “that such operations be carried out by the military forces of a sovereign or quasi-sovereign government.”<sup>9</sup> Because Hamas was neither a de jure nor a de facto sovereign and because its actions constituted terrorism (rather than warlike actions by a military force), the war exclusion did not apply. However, the Ninth Circuit remanded to the district court to determine whether Hamas’ actions fell under the third prong of the war exclusion for “insurrection, rebellion, or revolution.”

Recently, a federal district court in New York examined the scope of the war exclusion’s third prong for “insur-

rection.” In *Hartford Fire Ins. Co. v. Western Union Co.*, the policyholder, Western Union, sought coverage for losses arising out of an underlying lawsuit filed by the family of an American college student alleging that Western Union provided financial support to the Donetsk People’s Republic (“DPR”), a Russian-backed separatist group in Eastern Ukraine, who shot down a plane on which the student was a passenger.<sup>10</sup> The insurer denied coverage for the underlying lawsuit, relying on the policy’s war exclusion. In granting summary judgment to the insurer, the district court held that the underlying claim fell squarely within the meaning of “insurrection,” defined as “(1) a violent uprising by a group or movement (2) acting for the specific purpose of overthrowing the constituted government and seizing its powers.”<sup>11</sup> Because the DPR was in the midst of a violent uprising to overthrow the Ukrainian government and increase the Russian Federation’s control over territory in Eastern Ukraine, the court reasoned that the DPR’s downing of the plane, and the student’s death, arose out of an insurrection. Therefore, the policy’s war exclusion was deemed applicable.

No matter the specific war exclusion language utilized, however, courts have generally agreed that the war exclusion applies only to traditional or conventional forms of warfare.<sup>12</sup>

## II. The War Exclusion as Applied to Cyber Attacks: The *Merck* Decisions

The advent of the internet has made it possible for state-backed or unaffiliated actors to conduct cyberattacks on the networks of their victims, rendering their information inaccessible and operations useless. As cyberattacks have become more prolific, a question for courts has become: are the losses resulting from such attacks covered by insurance policies despite the presence of a war exclusion? In *Merck & Co., Inc. v. Ace Am. Ins. Co., et al.*, New Jersey courts answered the question in the affirmative.<sup>13</sup>

Merck & Co., Inc. (“Merck”), a multinational pharmaceutical company, was a victim of a cyber attack in June 2017 when a malware, known as NotPetya, infected Merck’s computer and network systems after Merck utilized a Ukrainian-based accounting software that was hacked. Forty thousand of Merck’s computers were infected, rendering them inoperable and causing massive disruptions to Merck’s operations, resulting in over \$1.4 billion in losses.

Merck submitted notice of its losses to its “all risk” property insurance policy program, consisting of eight insurers and twenty-six policies and providing a total of \$1.75 billion in limits. However, most of the insurers denied coverage on the basis that the policies’ hostile/warlike action exclusion applied, which purported to preclude coverage for:

Loss or damage caused by hostile or warlike action in time of peace or war, including action in hindering, combating, or defending against an actual, impending, or expected attack:

- (a) by any government or sovereign power (de jure or de facto) or by any authority maintaining or using military, naval, or air forces;
- (b) or by military, naval, or air forces;
- (c) or by an agent of such government, power, authority, or forces[.]

The insurers argued that the exclusion applied because the malware was introduced through a server located in Merck’s Ukrainian office that was running a Ukrainian-based accounting software and, therefore, the cyber-attack was likely orchestrated on behalf of actors working for the Russian Federation.

Merck filed suit in state court in New Jersey and, after extensive discovery, the parties submitted cross-motions for summary judgment on the applicability of the hostile/warlike action exclusion. The trial court granted summary judgment to Merck, finding that the plain language of the exclusion did not contemplate cyberattacks and applied only to traditional forms of warfare. The insurers appealed.

The appellate court began its analysis with a discussion of basic insurance coverage concepts under New Jersey law, including that: insurers bear the burden of establishing that exclusionary provisions apply; exclusionary provisions must be construed narrowly, and; ambiguous exclusionary provisions must be interpreted in favor of the insured. Indeed, the court noted that “experienced all risk insurers should [...] expect[] the exclusions drafted by them to be construed narrowly against them and should have calculated their premiums accordingly.”<sup>14</sup> As such, the insurers bore the heavy burden of establishing that the hostile/warlike action exclusion unambiguously

applied to the NotPetya cyberattack. In attempting to meet this burden, the insurers conceded that the cyberattack was not “warlike” and, instead, argued that the attack was a “hostile” action by a government or sovereign actor (i.e., the Russian Federation), with the term “hostile” being read in the broadest sense to mean reflecting “ill will or a desire to harm.”

The appellate court rejected the insurers’ interpretation, holding that the exclusion did not explicitly preclude coverage for government action motivated by “ill will.” Therefore, construing the exclusion narrowly, the court held that its plain language did not encompass cyberattacks on non-military companies providing accounting software for commercial purposes to non-military customers, like Merck, “regardless of whether the attack was instigated by a private actor or a ‘government or sovereign power.’”<sup>15</sup> The court also considered the history of the war exclusion, recognizing that no court had ever analyzed the issue of cyberattacks, but noting that “that similar exclusions have never been applied outside the context of a clear war or concerted military action.”<sup>16</sup> Accordingly, the court found that the insurers failed to satisfy their burden to show that the exclusion applied to the NotPetya cyberattack on Merck.

Following the appellate court’s decision, the insurers appealed to the New Jersey Supreme Court, New Jersey’s highest court.

On the eve of oral argument before the New Jersey Supreme Court, the parties settled, leaving intact the lower court’s ruling.<sup>17</sup>

### III. Recent Introduction of Cyberattack Exclusions

Likely in response to the *Merck* decisions, an increase in reported cyberattack claims, the increasing costs associated with cyber claims, and concern about future incidents, insurers have begun to introduce new war exclusions into the market.

For example, Lloyd’s of London issued Bulletin Y5381 in August 2022, setting forth a host of exclusions to be added by members of the Lloyd’s marketplace to standalone cyberattack policies, including exclusions for state backed cyberattacks.<sup>18</sup> The bulletin clarified that the cyberattack exclusions, at a minimum, must exclude “losses arising from war” and “losses arising from state backed cyber-attacks

that (a) significantly impair the ability of a state to function or (b) that significantly impair the security capabilities of a state.” The bulletin also required that exclusions be clear as to whether they cover computer systems “located outside any state which is affected [...] by the state backed cyber-attack” and how “any state backed cyber-attack will be attributed to one or more states.” Lloyd’s mandated that these exclusions be implemented for all policies otherwise covering cyberattacks, including at renewals, beginning March 31, 2023.

On May 14, 2024, Lloyd’s issued Bulletin Y5433 to provide clarification on the type of policy language to be used by insurers and reinsurers when offering cyberattack coverage, noting that some clauses could no longer be used because they were not considered sufficiently clear or robust.<sup>19</sup> For instance, one variant of the exclusion that is being phased out in 2025 contains the carve back for losses suffered as a result of cyberattacks carried out as part of war where the affected computer systems are located outside of the warring states.

The Lloyd’s approved clauses purport to exclude all state backed cyberattacks, both war and/or non-war related. However, Lloyd’s allows some carve-backs for coverage, including exclusions that only preclude coverage for losses arising out of “significant impairments from non-war.” In other words, some cyberattack exclusions will only apply where the “significant impairment” threshold is met and, if not, coverage is triggered.

For those Lloyd’s syndicates wishing to provide coverage “for cyber-attacks carried out as part of a conventional war [after January 1, 2025], [Lloyd’s has mandated that they] do so with a clear and distinct coverage grant, for example thorough a separate, affirmative product.” But, Lloyd’s has limited the ability to provide such coverage to “advanced” syndicates and only on renewal business.

While many Lloyd’s syndicates and non-Lloyd’s insurers have adopted the Lloyd’s cyberattack exclusions, other insurers, such as Beazley, have provided their own adaptations.<sup>20</sup>

In sum, these actions demonstrate the trend whereby insurers seek to introduce new exclusions to try to limit coverage.

#### IV. Take Aways

As the cyber insurance market evolves to protect policyholders against ever-changing risks, and in the absence of standard form policy language, it is clear that policyholders may face a plethora of varied war exclusions in their policies.

The *Merck* decision, and case law interpreting traditional war exclusions, have made clear that these exclusions “have never been applied outside the context of a clear war or concerted military action.”

As to new exclusions, courts faced with interpreting them will apply traditional rules of insurance policy interpretation. In short, this means that the burden of demonstrating the applicability of such exclusions, “a heavy one,” is on the insurer. Moreover, under such rules, exclusions will only be applied if they are clear and unambiguous, such that any ambiguity will be resolved in favor of the policyholder and against the insurer.

While this may give policyholders some degree of comfort, it is highly recommended that new exclusions be carefully vetted and discussed between policyholder and insurer so that both parties understand what the insurers are seeking to achieve with the introduction of new limitations on coverage. Given the lack of uniformity in the market, it may be possible for policyholders, with the help of insurance professionals, to renegotiate some of these provisions.

In addition, policyholders should carefully review their cyber, property, tech E&O, and other policies to see where such policies cover cyber risks as well as the means by which they might exclude them.

Ultimately, in the same way that cybersecurity requires vigilance with regard to threats, insurance professionals will need to remain alert to changes in the nature of how such risks are insured.

---

#### Endnotes

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

2. Katherine S. Wan, *Notpetya, Not Warfare: Rethinking the Insurance War Exclusion in the Context of International Cyberattacks*, 95 WASH. L. REV. 1595, 1600 (2020) (noting that the insurance industry decided to incorporate war exclusions instead of attempt to calculate premiums to accommodate war-related losses).
3. See *Merck & Co., Inc. v. Ace Am. Ins. Co., et al.*, in the Superior Court of New Jersey, Nos. A-1879-21, A-1882-21, at 24–25 (May 1, 2023).
4. See supra n. ii.
5. *Merck & Co., Inc.*, Nos. A-1879-21, A-1882-21, at 24–25.
6. See infra n. xii.
7. 929 F.3d. 1143 (9th Cir. 2019).
8. Courts from other jurisdictions agree. See e.g., *Holiday Inns, Inc. v. Aetna Ins. Co.*, 571 F. Supp. 1460 (S.D.N.Y. 1983) (in the insurance context, “war” must be “between sovereign or quasi-sovereign states”); *Pan Am. World Airways, Inc. v. Aetna Cas. & Surety Co.*, 505 F.2d 989, 1000 (2d Cir. 1974) (“war refers to and includes only hostilities carried on by entities that constitute governments at least de facto in character”).
9. *Id.*
10. 630 F. Supp. 3d 431 (S.D.N.Y. 2022).
11. Citing to the *Pan Am* decision in defining the term.
12. *Pan Am.*, 505 F.2d at 997–98 (war exclusion did not apply to plane hijacking because it was not a military plane hauling military cargo and the hijacker was not an agent for any nation at war); *Holiday Inns, Inc.*, 571 F. Supp. at 1460–1503 (war exclusion did not apply to damages to Beirut hotel caused by “civil commotions” rather than a war between sovereign states); *Stanbery v. Aetna Life Ins. Co.*, 26 N.J. Super. 498, 503 (Law Div. 1953) (war exclusion applied where decedent was killed in a mine explosion while serving in the United States army during the Korean War); *Diamond Shamrock Chems. Co. v. Aetna Cas. & Sur. Co.*, 258 N.J. Super. 167, 233–42 (App. Div. 1992) (war exclusion applied to settlement of class action brought by Vietnam veterans exposed to Agent Orange); *Queen Ins. Co. of Am. v. Globe & Rutgers Fire Ins. Co.*, 282 F. 976, 978–80 (2d Cir. 1922) (ship collision losses not covered by war risk policy because the ships were traveling in a convoy due to the presence of a war, even though the collision was caused by faulty navigation); *Int’l Dairy Eng’g Co. of Asia v. Am. Home Assurance Co.*, 352 F. Supp. 827, 828–31 (N.D. Cal. 1970), *aff’d*, 474 F.2d 1242 (9th Cir. 1973) (war exclusion applied to damage to milk processing plant in Saigon, Vietnam because the damage was caused by a parachute flare dropped by an airplane in connection with military operations).
13. Nos. A-1879-21, A-1882-21 (May 1, 2023); see also *See Merck & Co. v. Ace Am. Ins. Co.*, 2021 N.J. Super. Unpub. LEXIS 4566, \*1 (Dec. 6, 2021).
14. *Merck & Co., Inc.*, Nos. A-1879-21, A-1882-21 at 17.
15. *Id.* at 24.
16. *Id.* at 25.
17. P. Halprin, *Halprin in HealthcareInfoSecurity: How the Merck Case Shapes the Future of Cyber Insurance* (Jan. 11, 2024), <https://www.healthcareinfosecurity.com/interviews/how-merck-case-shapes-future-cyber-insurance-i-5345>.
18. Lloyd’s, Market Bulletin Y5381 – State-Backed Cyber-Attack Exclusions (2022), <https://assets.lloyds.com/media/35926dc8-c885-497b-aed86d2f87c1415d/Y5381%20Market%20Bulletin%20-%20Cyber-attack%20exclusions.pdf>.
19. Lloyd’s, Market Bulletin Y5433 – State-Backed Cyber-Attack Wordings (2024), <https://assets.lloyds.com/media/6335bcb0-e2a2-4378-8328-1ddf54828f2f/Y5433.pdf>.
20. L.S. Howard, *Lloyd’s Cyber War Exclusions: Confusing, Disruptive, but Necessary?* (May 9, 2023), <https://www.insurancejournal.com/news/international/2023/05/09/720020.htm#>. ■

**MEALEY'S: EMERGING INSURANCE DISPUTES**

*edited by Jennifer Hans*

**The Report** is produced twice monthly by



1600 John F. Kennedy Blvd., Suite 1655, Philadelphia, PA 19103, USA

Telephone: (215)564-1788 1-800-MEALEYS (1-800-632-5397)

Email: [mealeyinfo@lexisnexis.com](mailto:mealeyinfo@lexisnexis.com)

Web site: <http://www.lexisnexis.com/mealeys>

ISSN 1087-139X