THE YALE LAW JOURNAL FORUM
OCTOBER 15, 2019

Prove It! Judging the Hostile-or-Warlike-Action Exclusion in Cyber-Insurance Policies

Adam B. Shniderman

ABSTRACT. In late 2018, snack-food giant Mondelez International sued Zurich Insurance for improperly denying coverage for losses caused by the NotPetya computer virus. Zurich has asserted an exclusion for hostile and warlike actions by a sovereign or its agents. Zurich's exclusion argument is not atypical; many standalone cyber-insurance policies contain similar provisions. As a result, the case has garnered significant attention among insurance experts. This Essay explores the challenges facing insurers and insureds litigating denials of coverage under the hostile-or-warlike-action exclusion. The current legal framework is not up to the challenge. To assert the exclusion successfully, the insurer must demonstrate both that the act was perpetrated by a sovereign or its agent and that the act is hostile or warlike. Given the nature of cyberattacks, insurers and insureds face significant hurdles on both fronts. This Essay explores the significant difficulties of accurately determining the source of a hack, analyzes the implications for determining insurance coverage with respect to the hostile-or-warlike-action exclusion, and offers several novel proposals for improving cyberattack attribution and adjudicating coverage disputes.

INTRODUCTION

In 2017, multinational snack-food company Mondelez International was a victim of the NotPetya malware attacks.[1] That virus permanently disabled 1,700 of the company's servers and 24,000 of its laptops.[2] Its insurer, Zurich, denied coverage, asserting that the event fell within a policy exclusion for "hostile or warlike action . . . by any government or sovereign power . . . or agent or

1. Complaint at 2, Mondelez Int'l, Inc. v. Zurich Am. Ins. Co., No. 2018L011008, 2018 WL 4941760 (Ill. Cir. Ct. Oct. 10, 2018).

2. *Id.* at 3.

authority of [such a party]."[3] The case, now being litigated in Chicago, has garnered significant attention among insurance-law experts and scholars.[4]

The case is emblematic of the coverage battles likely to arise out of similar exclusions in many cyber-insurance policies.[5] Mondelez contends that Zurich's application of this exclusion is unprecedented, particularly for an event other than conventional armed conflict.[6] In court, Mondelez appears focused on the nature of the attack, rather than the identity of the perpetrator. However, the policy exclusion at issue has two important facets: who and why.

An insurer ordinarily must show by a preponderance of the evidence that an exclusion applies.[7] With respect to the hostile-or-warlike-action exclusion at issue in *Mondelez*, Zurich must make two showings. First, the insurer must show that a government or sovereign power, or its agent, is responsible for the attack. Second, the insurer must establish that the loss was a result of hostile or warlike action. As this Essay will demonstrate, meeting both demands will prove difficult in court.

This Essay explores the issues that insurers and insureds are likely to face in litigating these coverage disputes. Part I begins with a background discussion of

---

3. *Id.* at 3.

4. *See, e.g.*, Leonid Bershidsky, *Zurich Policyholder Dispute Highlights Danger of Calling Out Cyber Attackers: Opinion*, INS. J. (Jan. 11, 2019), https://www.insurancejournal.com/news/international/2019/01/11/514553.htm [https://perma.cc/2PLZ-PNFA]; Ariel E. Levite & Wyatt Hoffman, *A Moment of Truth for Cyber Insurance*, LAWFARE (Feb. 27, 2019, 9:21 AM), https://www.lawfareblog.com/moment-truth-cyber-insurance [https://perma.cc/B9AA-WVJP]; Peter Littlejohns, *The Mondelez Legal Case Could Have a Huge Impact on Cyber-Attack Insurance,* NS INS. (Jan. 17, 2019), https://www.nsinsurance.com/news/mondelez-zurich-cyber-attack-insurance [https://perma.cc/5H3R-DPRC].

5. *See* Lon Berk, *Sony Hack Will Bring Cyberinsurance to Forefront in 2015,* LAW360 (Jan. 2, 2015, 12:51 PM), https://www.law360.com/articles/607705/sony-hack-will-bring-cyberinsurance-to-forefront-in-2015 [https://perma.cc/E9JX-MKM8]. The policy issued to Mondelez that is the subject of the litigation is not, however, a standalone cyber policy. Rather, it is an all-risk property loss policy. Complaint, *supra* note 1, at 1. Notwithstanding the difference, the coverage provision at issue reflects language used in many standalone cyber policies.

6. Complaint, *supra* note 1, at 4.

7. *See, e.g.*, TEX. INS. CODE. ANN. art. 5, § 554.002 (West 2019) (providing that the insurer has the burden of proof as to exclusions in the insurance contract); Aydin Corp. v. First State Ins., 959 P.2d 1213, 1215 (Cal. 1998) ("[T]he burden is on the insurer to prove the claim is specifically excluded."); Hubred v. Control Data Corp., 442 N.W.2d 308, 310 (Minn. 1989) ("An insurer has the burden of proving a policy exclusion applies."); Continental Ins. v. Louis Marx & Co., 415 N.E.2d 315, 317 (Ohio 1980) ("[A] defense based on an exception or exclusion in an insurance policy is an affirmative one, and the burden is cast on the insurer to establish it.") (quoting Arcos Corp. v. Am. Mut. Liab. Ins., 350 F. Supp. 380, 384 (E.D. Pa. 1972)); Brown v. Snohomish Cty. Physicians Corp., 845 P.2d 334, 340 (Wash. 1993) ("When the insured makes the prima facie case that there is coverage, the burden is on the insurer to prove that the loss is not covered because of an exclusionary provision in the policy.").

the rise of cyber insurance and discusses the rationale for policy exclusions such as the one at issue in *Mondelez*. Part II explores the challenges associated with attributing a breach to a particular source. Part III discusses the problems associated with determining whether the attack constitutes a hostile or warlike action. Finally, Part IV offers several possible solutions in creating a legal regime capable of adjudicating these coverage disputes.

I. BACKGROUND ON CYBER INSURANCE

Through litigation and policy revisions, insurers have resoundingly demonstrated their unwillingness to provide coverage for cyber breaches under general liability policies, including the Commercial General Liability (CGL) policy—the insurance policy companies purchase to provide protection against a broad range of claims.[8] While insurers have yet to provide a clear reason for the denials of coverage, several factors drive their decisions.

First, insurers possess incomplete data on the probability and size of losses that could result from a cyberbreach. The "law of large numbers" undergirds risk-spreading, which incentivizes insurers to provide coverage.[9] The larger the pool of insured risks, the smaller the risk will be to everyone in the pool, on average.[10] Calculating the risk and being able to combine it with enough other similar risks is crucial to an insurer's remaining solvent.[11] As a result, insurers are hesitant to offer coverage "against events where the probability of an occurrence is ambiguous either because there are limited statistical data and/or experts have different theories as to underlying causal mechanisms."[12]

---

8. *See* Jeff Woodward, *The 2004 ISO CGL Policy*, IRMI: EXPERT COMMENT. (Apr. 2004), https://www.irmi.com/articles/expert-commentary/the-2004-iso-cgl-policy [https://perma.cc/BE45-2M3J]; Jeff Woodward, *The 2001 ISO CGL Revision*, IRMI: EXPERT COMMENT. (Jan. 2002), https://www.irmi.com/articles/expert-commentary/the-2001-iso-cgl-revision [https://perma.cc/97RZ-5K3H]; *see also, e.g.*, St. Paul Fire & Marine Ins. v. Rosen Millenium, Inc., 337 F. Supp. 3d 1176 (M.D. Fla. 2018); Innovak Int'l, Inc. v. Hanover Ins., 280 F. Supp. 3d 1340, 1347 (M.D. Fla. 2017); State Auto Prop. & Cas. Ins. v. Midwest Computs. & More, 147 F. Supp. 2d 1113 (W.D. Okla. 2001); Recall Total Info. Mgmt. v. Fed. Ins., 115 A.3d 458 (Conn. 2015); Zurich Am. Ins. Co. v. Sony Corp. of Am., No. 651982/2011, 2014 N.Y. Misc. Lexis 5141 (N.Y. Sup. Ct. Feb. 21, 2014).

9. TOM BAKER & KYLE D. LOGUE, INSURANCE LAW AND POLICY: CASES AND MATERIALS 4-5 (4th ed. 2017).

10. *Id*. at 5.

11. *See* Michelle E. Boardman, *Known Unknowns: The Delusion of Terrorism Insurance*, 93 GEO. L.J. 783, 784 (2005).

12. Robin M. Hogarth & Howard Kunreuther, *Pricing Insurance and Warranties: Ambiguity and Correlated Risks*, 17 GENEVA PAPERS ON RISK & INS. THEORY 35, 36 (1992).

Second, events that can produce large losses because the risks are correlated, as is the case with cyberattacks, compound insurers' concerns.[13] Correlated risk refers to the simultaneous occurrence of numerous losses from a single cause or event.[14] These risks, along with those very rare events for which the insurer cannot gather sufficient data to predict, create underwriting difficulties for insurers.[15] Actuarial data is either unavailable or indicates that premiums must be so high that consumers would choose not to purchase the insurance.[16]

Third, it is possible that cyberbreaches fall into a category of uninsurable phenomena.[17] For example, war and terrorism are frequently excluded from all lines of insurance coverage because they exhibit these challenges.[18] Indeed, "[w]ar creates the 'perfect storm' of actuarial nightmares: a correlated, catastrophic, ongoing clash event."[19] Terrorism occurs so rarely that insurers lack sufficient data to price insurance.[20] Insurers are left to price terrorism-insurance premiums based on best guesses regarding the likelihood and size of losses.[21] The federal government now reinsures terrorism risk due to the difficulties

---

13. *Id*.

14. Floods, earthquakes, hurricanes, nuclear disasters, and pollution are all routinely excluded from various insurance lines because the risks are highly correlated. These risks can bring area-wide, concentrated losses, undermining the risk-spreading and law of averages insurers use to make profit and ensure solvency. These risks are often handled via policy exclusions. *See* Howard Kunreuther, *The Role of Insurance in Managing Extreme Events: Implications for Terrorism Coverage*, 22 RISK ANALYSIS 427, 430 (2002). In the cyber realm, the interconnectedness of computer systems and the ubiquity of operating systems are sources of correlated risk. For example, the NotPetya malware exploited the update procedure of a Ukrainian software to infect computers in Russia, the United Kingdom, Norway, the Netherlands, and France within five hours of its first detection. Similarly, the WannaCry ransomware exploited a flaw in Windows 10 to infect computers across the globe. *Report: Insuring Cyber Risk*, LE CLUB DES JURISTES 25 (2018), https://www.leclubdesjuristes.com/wp-content/uploads/2018/01/cdj_insuring-cyber-risk_janvier_2018_uk.pdf [https://perma.cc/QU8B-TPKD].

15. *See* Boardman, *supra* note 11, at 784.

16. *See id*. at 812-14.

17. *See id*.

18. *Id*. at 784.

19. *Id*. at 833.

20. *See id*. at 784; *see also* Howard Kunreuther & Erwann Michel-Kerjan, Policy Watch, *Challenges for Terrorism Risk Insurance in the United States*, 18 J. ECON. PERSP. 201, 205 (2004) (describing the inherent difficulty in pricing insurance for acts of terrorism).

21. "An insurer must first answer how much it should set aside in reserve to meet all expected losses, and so how much it should charge for a given risk." Boardman, *supra* note 15, at 812. To achieve these goals, insurers rely on actuarial science, which uses statistical data about the risk of a loss to calculate appropriate premiums and ensure they have cash reserves to pay claims. In the absence of this data, insurers are left to rely on models that are poorly suited to estimate the risks of terrorism-related losses. *See* Kunreuther & Michel-Kerjan, *supra* note 20, at 205.

associated with appropriately pricing the insurance.[22] Cyberbreaches, being unpredictable, highly correlated, and costly, possess several of the qualities that make pricing coverage difficult.

The challenges in pricing cyberbreaches have led insurers to offer standalone cyber-insurance plans. Like all insurance policies, cyber policies contain exclusions rooted in insurers' judgments about risks they do not intend to cover. Specifically, cyber insurers have crafted exclusions for losses resulting from warlike actions, terrorism, and attacks by foreign enemies, governments, and sovereigns or their agents.[23] Implementing these exclusions in the cyber realm, however, is particularly difficult. Hackers can mask their identity, making it difficult to ascertain the source of a breach. Additionally, incomplete information makes it difficult to ascertain the purposes of a breach — whether criminal, terroristic, or warlike action. Thus, cyber insurers may pay for losses they did not intend to insure or deny payment for losses that should have been covered.

II. IDENTIFYING THE PERPETRATOR

The hostile-or-warlike-action exclusion hinges in part on the perpetrator's identity. Insurers can only claim the exclusion if a sovereign or its agent carries out the breach. As a result, determining an insured's right to coverage depends in large part on "attribution" — ascertaining the perpetrator's identity. The attribution problem raises significant technical and political challenges.[24] Hackers have myriad tools for hiding their identity. Even where the technical challenges can be overcome, governments may be reticent to identify the source of the attack for political reasons.[25]

A. Attribution Challenges

A core challenge of cyberattack attribution is evidentiary. Cyberattack attribution requires examining electronic evidence, including server logs, IP

22. Following the 9/11 attacks, the U.S. government enacted the Terrorism Risk Insurance Act (TRIA), which provides reinsurance to insurers for acts of terrorism that meet particular criteria. Terrorism Risk Insurance Act of 2002, Pub. L. No. 107-297, 116 Stat. 2322 (codified as amended in scattered sections of 12 U.S.C., 15 U.S.C., and 28 U.S.C.).

23. *See* Berk, *supra* note 5.

24. *See* Thomas Rid & Ben Buchanan, *Attributing Cyber Attacks*, 38 STRATEGIC STUD. 4 (2015).

25. *See* Kristen Eichensehr, *Risky Business: When Governments Do Not Attribute State-Sponsored Cyberattacks*, COUNCIL FOREIGN REL. (Oct. 4, 2016), https://www.cfr.org/blog/risky-business-when-governments-do-not-attribute-state-sponsored-cyberattacks [https://perma.cc/NDH3-WXCC].

addresses, other basic identifiers, and strings of code for digital signatures.[26] Even when sufficient electronic evidence can be gathered, it can be misleading.[27] Hackers have numerous technical tools to cover their tracks.[28] They can spoof their IP address—making it look like the hack emanated from another computer—use proxy servers to hide their original location, harness the computing power of numerous computers, or use any number of other tools that capitalize on the anonymity afforded by the internet's architecture.[29] Thus, even when investigators are able to gather what *appears* to be relevant evidence, significant hurdles remain. Given the current geopolitical climate, the true perpetrator may disguise its identity in a "false flag" operation—using technological means to frame another group or nation for a breach.[30]

The cyberattack at the opening of the 2018 Olympics in PyeongChang, South Korea illustrates these evidentiary issues. There, hackers "used a blend of techniques, tools, and practices that blended the fingerprints of threat groups connected to North Korea, China, and Russia."[31] Moreover, they routed traffic through North Korean IP addresses in an effort to mask their origin.[32] While Russia was initially believed to be the likely source, private security groups also suspected Chinese or North Korean hackers.[33]

---

26. *See* Rid & Buchanan, *supra* note 24, at 15-19.

27. *See* Jawwad A. Shamsi et al., *Attribution in Cyberspace: Techniques and Legal Implications*, 9 SECURITY COMM. NETWORKS 2886, 2892-94 (2016); Kim Zetter, *The Evidence That North Korea Hacked Sony Is Flimsy*, WIRED (Dec. 17, 2014, 5:32 PM), https://www.wired.com/2014/12/evidence-of-north-korea-hack-is-thin [https://perma.cc/9MXG-YV3M].

28. *See* Rajesh Kumar Goutam, *The Problem of Attribution in Cybersecurity*, INT'L J. COMPUTER APPLICATIONS, Dec. 2015, at 34, 35-36.

29. Shamsi et al., *supra* note 27, at 2888.

30. *See* Andy Greenberg, *Russian Hacker False Flags Work—Even After They're Exposed*, WIRED (Feb. 27, 2018, 1:01 PM), https://www.wired.com/story/russia-false-flag-hacks [https://perma.cc/78PF-R8S7]; Jasper Hamill, *Cyber-Security Expert Warns of 'False Flag' Digital Attacks*, FORBES (July 31, 2014), https://www.forbes.com/sites/jasperhamill/2014/07/31/cyber-security-expert-warns-of-false-flag-digital-attacks [https://perma.cc/28YL-74S9]; Steve Ranger, *False Flags, Red Herrings and Wild Goose Chases: Why Unmasking Hackers Is Harder Than Ever*, ZDNET (June 18, 2015, 6:07 PM), https://www.zdnet.com/article/false-flags-red-herrings-and-wild-goose-chases-why-unmasking-hackers-is-harder-than-ever [https://perma.cc/Y6YR-EQ4M].

31. Sean Gallagher, *Russia Accused of "False Flag" Attack on Olympic Opening*, ARS TECHNICA (Feb. 26, 2018, 5:22 PM), https://arstechnica.com/information-technology/2018/02/russia-accused-of-false-flag-attack-on-olympic-opening [https://perma.cc/6MST-WHVS].

32. *Id.*

33. *Id.*

In addition to its evidentiary challenges, attribution has become a geopolitical issue.[34] Nations have competing incentives when publicly attributing cyberattacks. On the one hand, there is a significant incentive to exercise restraint.[35] Governments must consider the potential for unwanted escalation or strained diplomatic relations resulting from publicly accusing another sovereign state.[36] Restraint is particularly important given the technical difficulties of accurately attributing cyberattacks. Even physical attacks can be difficult to attribute, and governments are unlikely to ever be one hundred percent certain of an attribution. Cyberattackers, however, actively seek to mask their identities and misdirect investigators — making accurate attribution even more difficult. On the other hand, states also have significant incentives for exaggerating their technical prowess by publicly attributing an attack even in the face of uncertainty.[37] For example, identifying the source of an attack can promote deterrence. A state launching a cyberattack will be forced to consider the ramifications knowing, or at least believing, that its identity will be discovered.

B. Classified Information in Attribution Disputes

The presence of classified information also presents challenges to attribution. Governments attributing cyberattacks often rely on classified information. In *Mondelez* and similar cases in the future, the insurer could be left with only press releases, news reports, and bare assertions regarding the perpetrator's identity. Private insurers may be unable to muster meaningful evidence in support of their assertions that a sovereign was responsible for an attack.

The 2014 Sony Pictures hack exemplifies the kind of public/private disagreement resulting from this information asymmetry. Hackers took over Sony's internal computer system and released stolen data, including personal information about employees, internal emails, executive salaries, and copies of unreleased films and scripts.[38] Shortly after the breach, the FBI confirmed that it was

---

34. Lily Hay Newman, *Hacker Lexicon: What Is the Attribution Problem?*, WIRED (Dec. 24, 2016, 7:00 AM), https://www.wired.com/2016/12/hacker-lexicon-attribution-problem [https://perma.cc/V2HB-N6LY].

35. *See* Sasha Romanosky, *Private-Sector Attribution of Cyber Attacks: A Growing Concern for the U.S. Government?*, LAWFARE (Dec. 21, 2017, 11:20 AM), https://www.lawfareblog.com/private-sector-attribution-cyber-attacks-growing-concern-us-government [https://perma.cc/4TSW-2EJU].

36. *Id.*

37. Benjamin Edwards et al., *Strategic Aspects of Cyberattack, Attribution, and Blame*, 114 PROC. NAT'L ACAD. SCI. 2825, 2826 (2017).

38. *See* Sean Fitz-Gerald, *Everything That's Happened in the Sony Leak* Scandal, VULTURE (Dec. 22, 2014), https://www.vulture.com/2014/12/everything-sony-leaks-scandal.html [https://

investigating the incident.[39] As information leaked, North Korea denied any involvement, but commended the attack as a righteous deed.[40] The nation had previously expressed its displeasure with Sony's planned release of *The Interview*, a satirical film about the assassination of the North Korean leader.[41]

Relying on confidential information, a U.S. official stated nearly a month after the breach that North Korea was indeed the culprit.[42] The FBI confirmed this attribution shortly thereafter, marking the first time a government agency had formally blamed a foreign government for a cyberattack.[43] In a statement, the FBI announced that "in close collaboration with other U.S. government departments and agencies, the FBI now has enough information to conclude that the North Korean government is responsible for these actions."[44] Despite these assertions, many remained skeptical of the evidence.[45]

---

perma.cc/R4W7-QGLN]; *see also* Steven Musil, *Sony Hack Leaked 47,000 Social Security Numbers, Celebrity Data*, CNET (Dec. 4, 2014, 7:05 PM), https://www.cnet.com/news/sony-hack-said-to-leak-47000-social-security-numbers-celebrity-data [https://perma.cc/MQ5S-969Y] (explaining the data stolen from the Sony breach); Aly Weisman, *Leaked: Hacked Sony Docs Reveal Top 17 Executives' Multimillion-Dollar Salaries*, BUS. INSIDER (Dec. 2, 2014, 10:52 AM), https://www.businessinsider.com/hacked-sony-docs-top-execs-paychecks-2014-12 [https://perma.cc/HY2U-CXKJ] (same).

39. Aly Weisman, *A Timeline of the Crazy Events in the Sony Hacking Scandal*, BUS. INSIDER (Dec. 9, 2014, 4:15 PM), https://www.businessinsider.com/sony-cyber-hack-timeline-2014-12 [https://perma.cc/A9LL-EGP2].

40. Ben Child, *North Korea Says Sony Cyber-Attack May Be 'Righteous' Work of Its Supporters*, GUARDIAN (Dec, 8, 2014, 7:32 AM), https://www.theguardian.com/film/2014/dec/08/north-korea-sony-cyber-attack-the-interview [https://perma.cc/V3BE-68NS].

41. Ben Beaumont-Thomas, *North Korea Complains to UN About Seth Rogen Comedy* The Interview, GUARDIAN (July 10, 2014, 3:37 AM), https://www.theguardian.com/film/2014/jul/10/north-korea-un-the-interview-seth-rogen-james-franco [https://perma.cc/772Q-28WC].

42. David E. Sanger & Nicole Perlroth, *U.S. Said to Find North Korea Ordered Cyberattack on Sony*, N.Y. TIMES (Dec. 17, 2014), https://www.nytimes.com/2014/12/18/world/asia/us-links-north-korea-to-sony-hacking.html [https://perma.cc/772Q-28WC].

43. Ellen Nakashima, *U.S. Attributes Cyberattack on Sony to North Korea*, WASH. POST (Dec. 19, 2014), https://www.washingtonpost.com/world/national-security/us-attributes-sony-attack-to-north-korea/2014/12/19/fc3aec60-8790-11e4-a702-fa31ff4ae98e_story.html [https://perma.cc/WH85-UAMD].

44. *Update on Sony Investigation*, FED. BUREAU INVESTIGATION (Dec. 19, 2014), https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation [https://perma.cc/9N5S-KFG9].

45. *See* Andy Greenberg, *FBI Director: Sony's "Sloppy" North Korean Hackers Revealed Their IP Addresses*, WIRED (Jan. 7, 2015, 1:51 PM), https://www.wired.com/2015/01/fbi-director-says-north-korean-hackers-sometimes-failed-use-proxies-sony-hack [https://perma.cc/AXY5-ZNMC]; Tal Kopan, *U.S.: No Alternate Leads in Sony Hack*, POLITICO (Dec. 29, 2014, 7:41 PM), https://www.politico.com/story/2014/12/fbi-briefed-on-alternate-sony-hack-theory-113866 [https://perma.cc/N4FX-JJMY].

Several weeks later, the FBI met with experts from the private security firm Norse.[46] The company made its case that North Korea was *not* responsible for the hack. Norse shared information it believed supported the theory that several individuals, including a former Sony employee, were behind the attack.[47] The FBI maintained its position that the North Korean government was responsible.[48] It refused to share information with Norse, citing a need to protect sources and methods.[49] Lending increased credibility to the FBI's attribution, the *New York Times* would later reveal that the NSA had breached North Korea's networks prior to the attack.[50]

While private companies have narrowed the gap with the government in their abilities to conduct postattack investigations, they remain at an informational disadvantage.[51] The government has a monopoly on the intelligence community capabilities that assist in attribution.[52] The NSA collects vast amounts of signals intelligence, intercepting foreign communications and hacking foreign adversaries.[53] The FBI and Secret Service engage in similar activities domestically.[54] These and other intelligence and law-enforcement agencies can rely on information unavailable to the private sector to inform diplomatic and military responses to cyberattacks. The Obama Administration made executive and legislative efforts to increase information sharing, but further transparency faces a number of hurdles.[55]

The attribution problem poses significant problems for the hostile-or-warlike-action exclusion. Insurance coverage requires private actors to indemnify

---

46. Anu Passary, *FBI Refuses to Acknowledge Sony Pictures Hacking May Be Insider Job*, TECH TIMES (Dec. 31, 2014, 7:31 AM), https://www.techtimes.com/articles/23946/20141231/fbi-refuses-to-acknowledge-sony-pictures-hacking-may-be-insider-job.htm [https://perma.cc/59W2-QTXL].

47. *Id*.

48. Kopan, *supra* note 45.

49. Pamela Brown & Mary Kay Mallonee, *North Korea Did It: FBI Not Budging on Sony Hack Culprit*, CNN (June 4, 2015, 9:40 PM), https://www.cnn.com/2014/12/30/justice/fbi-sony-hack/index.html [https://perma.cc/P4J5-SWHW].

50. David E. Sanger & Martin Fackler, *N.S.A. Breached North Korean Networks Before Sony Attack, Officials Say*, N.Y. TIMES (Jan. 18, 2015), https://www.nytimes.com/2015/01/19/world/asia/nsa-tapped-into-north-korean-networks-before-sony-attack-officials-say.html [https://perma.cc/FR66-9Q35].

51. *See* Robert K. Knake, *Sharing Classified Cyber Threat Information with the Private Sector*, COUNCIL FOREIGN REL. (May 15, 2018), https://www.cfr.org/report/sharing-classified-cyber-threat-information-private-sector [https://perma.cc/QA9P-6EHH].

52. *Id.*

53. *Id*.

54. *Id*.

55. *Id*.

the insured for losses, without complete access to information. Hackers expertly cover their tracks, and the government will resist disclosing any classified information regarding its attribution.[56] Thus, an adequate framework must solve both aspects of the problem—correctly identifying the perpetrator and protecting the classified information that led to the identification.

With the burden on the insurer to support its assertion of a policy exclusion, how could a court or jury find for the insurer? Should the insured bear the burden of proving coverage? Ordinarily, the insured must make only a prima facie showing of coverage.[57] The insurer then bears the burden of establishing the applicability of an exclusion by a preponderance of the evidence.[58] The insurer, however, will have incomplete information about the source of the attack. If a case involves classified intelligence, the government will assert the state secrets privilege and courts will dismiss coverage disputes.[59] This process will make insurers the de facto final word on coverage. Reputational harm to insurers from repeated, wrongful denials of coverage would be insured's only protection from overzealous and improper application of the exclusion.

---

56. Indeed, if hauled into court to provide evidence in a coverage dispute, the government could assert the state secrets privilege. *See infra* notes 87-93 and accompanying text (discussing the scope and impact of the state secrets privilege). In a different context, the government has resisted disclosing the "network investigative techniques" used to identify individuals engaged in criminal activity. *See* Rupinder K. Garcha, *NITS a No-Go: Disclosing Exploits and Technological Vulnerabilities in Criminal Cases*, 93 N.Y.U. L. Rev. 822 (2018).

57. *See, e.g.*, Brown v. Snohomish Cty. Physicians Corp., 845 P.2d 334, 340 (Wash. 1993) ("When the insured makes the prima facie case that there is coverage, the burden is on the insurer to prove that the loss is not covered because of an exclusionary provision in the policy.").

58. *See supra* note 7.

59. According to the Fourth Circuit, "If a proceeding involving state secrets can be fairly litigated without resort to the privileged information, it may continue." El-Masri v. United States, 479 F.3d 296, 306 (4th Cir. 2007). However, "a proceeding in which the state secrets privilege is successfully interposed *must* be dismissed if the circumstances make clear that privileged information will be so central to the litigation that any attempt to proceed will threaten that information's disclosure." *Id.* at 308 (emphasis added). Three circumstances *require* dismissal: (1) the plaintiff cannot prove the prima facie elements of the claim without privileged evidence; (2) the defendants cannot properly defend themselves without the privileged evidence; (3) continued litigation poses an unjustified risk of disclosure. Wever v. AECOM Nat'l Sec. Programs Inc., No. 1:17-cv-00200, 2017 WL 5139263, at *6 (E.D. Va. June 15, 2017). The court's dismissal in *Wever* makes clear that the same analysis applies to cases in which the government is not a party. In a coverage dispute, the insured could present evidence from a private security firm indicating the breach was *not* perpetrated by or at the behest of a foreign government. Thus, the second scenario described above is most probable—the insurer's ability to adequately defend the claim by asserting the policy exclusion as an affirmative defense will be impaired.

III. CLASSIFYING THE ATTACK

The hostile-or-warlike-action exclusion also hinges on the nature of the attack. The terms "hostile" and "warlike" are not self-defining, and courts have interpreted them as having independent meaning. In addition to the identity of the attacker, the warlike-action exception is concerned with the nature of the attack. *Pan American World Airways v. Aetna Casualty and Surety Co.*[60] is the leading case interpreting the exclusion of "warlike action." In that case, a Pan Am jet was hijacked and destroyed by a group working for the Popular Front for the Liberation of Palestine (PFLP). The district court determined that the hijacking was "designed to serve as a spectacular display, as a round of 'symbolic blows,' as propaganda of a vividly compelling sort."[61] Due to the purpose of the attack, the district court reasoned that the act was not intended to be an act of war or a warlike operation against the United States or Israel. Additionally, because a state actor did not carry out the attacks, the hijacking did not fall within the policy exclusion, so the insurer had to pay.

On appeal, the Second Circuit affirmed the district court's ruling. The Second Circuit explained that courts interpret the warlike-action exclusion "in accordance with the ancient international law definition: war refers to and includes only hostilities carried on by entities that constitute governments at least de facto in character."[62] The Second Circuit also agreed that the PFLP's actions did not constitute "'warlike operation[s]' 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, particularly when the purpose is propaganda."[63]

Although *Pan Am* is instructive, it merely provides guidance on what actions *do not* constitute a warlike action. *Pan Am* left unanswered, however, the question of which elements *do*. Must an action be taken in furtherance of a "legitimate military objective"[64] to be warlike?

The *Mondelez* case shows the difficulty in litigating cyber-insurance disputes absent a clear list of elements for the warlike-action exclusion. For example, does

---

60. 368 F. Supp. 1098 (S.D.N.Y. 1973).

61. *Id.* at 1116 (footnote omitted).

62. Pan Am. World Airways, Inc. v. Aetna Cas. & Surety Co., 505 F.2d 989, 1012 (2d Cir. 1974).

63. *Id.* at 997.

64. The Geneva Conventions governing the conduct of war state that "[a]ttacks shall be limited strictly to military objectives . . . . [M]ilitary objectives are limited to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction . . . offers a definite military advantage." Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, June 8, 1977, 1125 U.N.T.S. 3. Thus, war is ordinarily defined as limited to legitimate military objectives.

a breach need to occur "near the site of warfare" to trigger the exception? The Second Circuit's opinion in *Pan Am* could be used to support the claim that it does.[65] Of course, unlike traditional warfare, the "site of warfare" for a cyberbreach presents a number of issues, the most obvious being the lack of a clear geographic area of conflict. Even if courts determine that "sites of warfare" are independent of physical location for the purposes of cyberattacks, insurers may be able to sidestep these thorny issues by invoking the hostile-act exclusion instead.

Courts have offered little guidance on the insurance meaning of the term "hostile act." They may turn to a variety of sources, including the dictionary, to determine its meaning. Merriam-Webster's dictionary defines "hostile" as (1) "of or relating to an enemy" or (2) "marked by malevolence: having or showing unfriendly feelings."[66]

A broad interpretation of "hostile act" could lead to controversial exclusions. For example, Chinese hackers have engaged in acts that may qualify, breaching biotechnology, mining, pharmaceutical, professional services, and transportation firms for years.[67] Chinese government hackers' theft of intellectual property is on the rise.[68] These actions are often characterized as "economic espionage" against the United States.[69] Despite their destructive effects, these hacks seem to meet the insurance definition of "warlike actions" less clearly than do breaches intended to infect and cripple computer systems, as happened to Mondelez. Under a broad interpretation of "hostile act," however, the theft of intellectual property via government-backed cyberintrusion could be excluded from coverage. Indeed, courts could quite reasonably conclude that the theft is "marked by malevolence."[70]

Ultimately, a broad interpretation of the hostile-or-warlike-action exclusion could prove problematic. An expansive interpretation of "hostile act" may leave

---

65. *See Pan Am. World Airways Inc.*, 505 F.2d at 1012.

66. *Hostile*, MERRIAM-WEBSTER DICTIONARY, https://www.merriam-webster.com/dictionary/hostile [https://perma.cc/5K27-XAL9]. The Oxford English Dictionary defines "hostile" as, "[o]f, pertaining to, or characteristic of an enemy; pertaining to or engaged in actual hostilities;" and "[o]f the nature or disposition of an enemy; unfriendly." *Hostile*, OXFORD ENG. DICTIONARY, https://www.oed.com/view/Entry/88770 [https://perma.cc/5G5Z-8WEJ].

67. Ken Dilanian, *China's Hackers Are Stealing Secrets from U.S. Firms Again, Experts Say*, NBC NEWS (Oct. 19, 2018 8:29 AM), https://www.nbcnews.com/news/china/china-s-hackers-are-stealing-secrets-u-s-firms-again-n917836 [https://perma.cc/FW2P-5ZWA].

68. *Id.*

69. Chris Bing, *U.S. Warns of 'Emerging' Global Cyber-Espionage Campaign by Chinese Hackers*, CYBERSCOOP (Apr. 28, 2017), https://www.cyberscoop.com/u-s-warns-emerging-global-cyber-espionage-campaign-chinese-hackers [https://perma.cc/8TD2-FKAH].

70. *See Hostile*, *supra* note 66.

little remaining coverage. For instance, coverage might only exist for accidental disclosures, which are already covered by other policies.[71] An insured could argue that its policy provides "illusory coverage"—excluding the very losses it appears to cover. Indeed, the standalone cyber-insurance policy developed as a response to the coverage gaps arising out of insurers' refusal to insure cyberbreaches in general liability policies. Yet their policy exclusions are worded in a way that, especially if read broadly, may leave many of those gaps unfilled. And if an insured were to succeed in an illusory coverage claim, the court could reform the policy to bring it into alignment with the insured's reasonable expectations.[72] In such a case, the insurer would be forced to pay a claim for which it had not taken actuarial account.

IV. FOUR AVENUES FOR REFORM

This Part considers several solutions from the cybersecurity and national security literature to assess whether they could alleviate the cyber-insurance market's difficulties. First, the government could create an entity akin to the National Transportation Safety Board (NTSB) to attribute cyberattacks. Second, the government could expand the Classified Information Procedures Act (CIPA) to apply in civil trials, and/or employ the Silent Witness Rule (SWR) to address the difficulties associated with using classified information in attributing cyberattacks. Third, courts could shift the burden of proving an exclusion's applicability from the insurer to the insured. Fourth, the government could create a national security court capable of handling, among other important issues, insurance-coverage disputes involving sensitive national security information. This would allow the state to avoid the classified-information problem as well as the foreign-policy issues related to publicly adjudicating cyber-insurance disputes.

A. The National Cybersecurity Safety Board

Over the last few years, there has been increasing support for the creation of a cybersecurity entity modeled on the NTSB.[73] The NTSB, which is responsible

71. *See* Travelers Indem. Co. Am. v. Portal Healthcare Sols., L.L.C., 644 F. App'x 245 (4th Cir. 2016) (discussing Portal's CGL coverage for accidental publication of patients' medical records online).

72. *See, e.g.*, Monticello Ins. v. Mike's Speedway Lounge, Inc., 949 F. Supp. 694, 696 (S.D. Ind. 1996) ("If the policy is illusory, then the Court must then determine whether [the policyholder] had a reasonable expectation that claims such as [the] cause of action [for which the policyholder is seeking coverage] would be covered by the policy.").

73. Scott J. Shackelford & Austin E. Brady, *Is It Time for a National Cybersecurity Safety Board? Examining the Policy Implications and Political Pushback*, 28 ALB. L.J. SCI. TECH. 56, 57-58 (2018).

for determining the causes of all civil-aviation accidents and significant accidents involving other forms of transportation,[74] focuses exclusively on investigation, rather than oversight.[75] It lacks any enforcement authority.[76] Nonetheless, according to some, the Board plays a crucial role in improving air safety.[77] Its success has led to proposals for the creation of an analogous independent government agency responsible for investigating cyberbreaches.

In 2014, an NSF Cybersecurity Ideas Lab group suggested creating an NTSB analogue charged with analyzing cybersecurity incidents and providing public reports on the circumstances and causes of each.[78] This agency could also cooperate with law-enforcement and national security agencies, assist with post-incident investigations, and make policy recommendations.[79] In a 2017 report, the Center for Strategic and International Studies suggested that a body modeled on the NTSB or the Federal Aviation Authority's Aviation Safety Reporting System could give companies an opportunity to report cyberbreaches without fear of regulatory repercussions.[80]

In 2018, Scott Shackelford and Austin Brady expanded on these calls for the creation of a National Cybersecurity Safety Board (NCSB).[81] Its purpose, they argue, would be to attribute cyberattacks and offer guidance to prevent future attacks. They called for the NCSB to investigate beyond the technical causes, examining the institutional culture issues that lead to being the victim of a data breach.[82]

There may, however, be impediments to the success of an NCSB. Shackelford and Brady overlook, or at least underestimate, the incentive to litigate the

---

74. *The Investigative Process*, NAT'L TRANSP. SAFETY BOARD, https://www.ntsb.gov/investigations/process/Pages/default.aspx [https://perma.cc/MF83-4XP9].

75. Erin Mundahl, *Does Cybersecurity Need an NTSB-Style Board?*, GOV'T TECH. (May 15, 2018), http://www.govtech.com/pcio/articles/Is-It-Time-for-a-NTSB-Style-Cybersecurity-Board.html [https://perma.cc/CEY4-LK2J].

76. *Id*.

77. *See* Clinton V. Oster Jr. et al., *Analyzing Aviation Safety: Problems, Challenges, Opportunities*, 43 RES. TRANSP. ECON. 148, 149 (2013).

78. Cybersecurity Ideas Lab, *Interdisciplinary Pathways Towards a More Secure Internet*, NAT'L SCI. FOUND., 21-23 (July 2014), https://www.nsf.gov/cise/news/CybersecurityIdeasLab_July2014.pdf [https://perma.cc/G6AW-SHWG].

79. *Id.* at 22.

80. CSIS Cyber Policy Task Force, *From Awareness to Action: A Cybersecurity Agenda for the 45h President*, CTR. STRATEGIC & INT'L STUD. 12 (2017), https://www.whitehouse.senate.gov/imo/media/doc/2016-01-03%20-%20CSIS%20Lewis%20Cyber%20Recommendations%20Next%20Administration.pdf [https://perma.cc/7P56-T9DY].

81. Shackelford & Brady, *supra* note 73, 61-68.

82. *Id*. at 62.

attribution of cyberattacks. Hundreds of millions of dollars may be at stake in an attribution.[83] Should litigation arise, the NCSB would do little to aid in adjudicating coverage disputes, particularly if the board relies on classified information to attribute attacks. While the creation of an NCSB may result in long-term, widespread changes in cybersecurity practices and may even alleviate some of the attribution challenges, the agency is insufficient to address the litigation troubles that will undoubtedly arise. The following proposals provide jurisprudential solutions that more directly address the difficulty of adjudicating coverage disputes.

B. The Classified Information Procedures Act

Protecting sensitive intelligence information from public disclosure is important for effectively adjudicating cyber-insurance coverage disputes. Currently, CIPA only protects classified information in criminal trials.[84] The Act provides a number of measures to keep classified documents and information out of the public record and, sometimes, out of the defendant's hands. Those measures include substituting both unclassified summaries of relevant documents and materials, and unclassified statements that admit the relevant facts.[85] Courts have supplemented CIPA with the judicially created SWR, which allows a witness to testify in code regarding sensitive information, with the parties and the jury given the key.[86] There is no equivalent law or set of procedures to address the use of classified information in civil cases.[87]

---

83. *See supra* Section II.A and accompanying notes.

84. Harry Graver, *The Classified Information Procedures Act: What It Means and How It's Applied*, LAWFARE (Nov. 20, 2017, 9:00 AM), https://www.lawfareblog.com/classified-information-procedures-act-what-it-means-and-how-its-applied [https://perma.cc/VC2D-6GCZ]. CIPA was designed, primarily, to prevent criminal defendants from engaging in graymail—the threatened exposure of classified information by a defendant unless charges are dropped.

85. *Id*. The ability to withhold evidence under CIPA is subject to the constraints of the Federal Rules of Criminal Procedure, *Brady v. Maryland*, 373 U.S. 83 (1963) (requiring the disclosure of exculpatory evidence by the government to a defendant), and the Jencks Act, 18 U.S.C. § 3500 (2018), which governs the disclosure of prior statements by witnesses called to testify at trial.

86. *See* United States v. Rosen, 520 F. Supp. 2d 786 (E.D. Va. 2007). For example, the court may replace the name of one city with Place *A* and another with Place *B*. The parties and the jury would be given the corresponding city names, but the public record and the witnesses' testimonies would simply include references to Place *A* and Place *B*.

87. Ian MacDougall, *CIPA Creep: The Classified Information Procedures Act and Its Drift into Civil National Security Litigation*, COLUM. HUM. RTS. L. REV., Winter 2014, at 668, 670.

Expanding CIPA to civil cases could allow parties to litigate coverage disputes more fully.[88] Currently, the state secrets privilege is the government's only method of protecting sensitive information in civil cases.[89] Unlike CIPA, the state secrets privilege does not preserve the classified nature of evidence and permit its use at trial.[90] Instead, the court must merely decide whether the information qualifies as a state secret, and if so, it excludes the evidence.[91] As a result of those evidentiary rulings, many civil cases involving alleged state secrets are dismissed.[92] By adopting a CIPA analogue for the civil context, the federal government could provide information regarding its attribution while shielding highly sensitive information from the public.[93]

Despite the allure of the CIPA, it may not provide a perfect solution. First, CIPA requires the recipient of the information to have a security clearance.[94] This process could lead to significantly increased litigation costs and delays.[95] Under

---

88. *See supra* notes 56-59 and accompanying text (discussing the likely impact of the state secrets privilege on coverage disputes).

89. *See* MacDougall, *supra* note 87, at 670-72.

90. *Is the State Secrets Privilege Too Powerful?*, NAT'L SECURITY L. BRIEF (Nov. 23, 2013), https://nationalsecuritylawbrief.com/2013/11/23/is-the-state-secrets-privilege-too-powerful [https://perma.cc/EX7R-LBXQ].

91. TODD GARVEY & EDWARD C. LIU, CONG. RESEARCH SERV., R41741, THE STATE SECRETS PRIVILEGE: PREVENTING THE DISCLOSURE OF SENSITIVE NATIONAL SECURITY INFORMATION DURING CIVIL LITIGATION 1 (2011).

92. *See* Margaret B. Kwoka, *The Procedural Exceptionalism of National Security Secrecy,* 97 B.U. L. REV. 103, 117-25 (2017); Daniel R. Cassman, Note, *Keep It Secret, Keep It Safe: An Empirical Analysis of the State Secrets Doctrine*, 67. STAN. L. REV. 1173 (2015); *see also* Project on Gov't. Secrecy, *The State Secrets Privilege: Selected Case Files*, FED'N AM. SCIENTISTS, https://fas.org/sgp/jud/statesec [https://perma.cc//VNN2-BMYP] (collecting cases in which the government has asserted the privilege and that subsequently have been dismissed).

93. CIPA provides a number of methods for protecting classified information. For example, under Sections 5 and 6, which govern the use of classified information in the defendant's possession, the government may propose that any classified evidence the court deems admissible be substituted with "a statement admitting relevant facts the classified information would tend to prove" or "the substitution for such classified information of a summary of the specified classified information." 18 U.S.C. app. III § 6(c)(1) (2018). The government's motion for substitution should be granted if the "statement or summary will provide the defendant substantially the same ability to make his defense as would disclosure of the specified classified information." *Id*. § 6(c).

94. GARVEY & LIU, *supra* note 91, at 3-4.

95. The estimated cost of issuing each such clearance is $5,596. Lindy Kyzer, *How Much Does a Security Clearance Cost?*, CLEARANCEJOBS (Aug. 27, 2018), https://news.clearancejobs.com/2018/08/27/how-much-does-a-security-clearance-cost [https://perma.cc/M7SR-WW8H]. Additionally, because of the resources required and the number of clearances issued, there is a delay of more than a year for Top Secret clearances. Loren Thompson, *One-Year Waits for Security Clearances Are Costing Washington Billions*, FORBES (May 23, 2017, 12:42 PM),

a CIPA-like regime, the government would have to clear either the parties' representatives, their counsel, or both in order to divulge the classified information. Even where repeat players are involved, the nature of modern litigation is such that insureds retain many different law firms. The government would need to clear these lawyers on an ad hoc basis or require that previously cleared counsel be appointed.[96] In addition to the administrative difficulties, CIPA's clearance requirement has been criticized for allowing courts to prevent defendants from seeing evidence in their own cases.[97] Indeed, CIPA allows the court to "issue protective orders prohibiting cleared counsel from sharing any classified information with the defendant."[98] One case, *United States v. Yunis*, provides "[a] stark example of [the] leeway granted to the government . . . . [T]he court held after an ex parte review of the information . . . that the defendant was not entitled to his own tape-recorded statements because they were not 'helpful to the defense of [the] accused.'"[99] These concerns are less significant, however, in the insurance-coverage context. The government will not be a party to these lawsuits. And these cases merely involve disputes over money.

Second, the government may object to the use of classified information even if a court finds the substituted unclassified summaries inadequate.[100] If the court determines that a substitution under CIPA § 6(c) is inadequate, it enters a disclosure order.[101] The Attorney General, however, has the authority to oppose the use of the classified information. Were the Attorney General to oppose a court's disclosure order, the court might sanction the government—"striking all or part of a witness'[s] testimony, resolving the issue of fact against the United States, or dismissing part or all of the indictment."[102] Thus, expanding CIPA may

https://www.forbes.com/sites/lorenthompson/2017/05/23/one-year-waits-for-security-clearances-are-costing-washington-billions [https://perma.cc/376X-8M74].

96. *See id*.

97. *See* Ellen Yaroshefsky, *Secret Evidence is Slowly Eroding the Adversary System: CIPA and FISA in the Courts*, 34 HOFSTRA L. REV. 1063, 1068 (2006).

98. TODD GARVEY & EDWARD C. LIU, CONG. RESEARCH SERV., R41742, PROTECTING CLASSIFIED INFORMATION AND THE RIGHTS OF CRIMINAL DEFENDANTS: THE CLASSIFIED INFORMATION PROCEDURES ACT 3 (2012).

99. Saul M. Pilchen & Benjamin B. Klubes, *Using the Classified Information Procedures Act in Criminal Cases: A Primer for Defense Counsel*, 31 AM. CRIM. L. REV. 191, 198 (1994) (emphasis omitted) (citing United States v. Yunis, 867 F.2d 617, 623 (D.C. Cir. 1989)).

100. GARVEY & LIU, *supra* note 91, at 6.

101. *2054. Synopsis of Classified Information Procedures Act (CIPA)*, U.S. DEP'T JUST., https://www.justice.gov/jm/criminal-resource-manual-2054-synopsis-classified-information-procedures-act-cipa [https://perma.cc/TBM8-V9VL].

102. *Id.*; *see also* United States v. Wilson, 586 F. Supp. 1011, 1013 (S.D.N.Y. 1984) ("If specified classified information is admissible, the Court may consider an alternative . . . . [I]f no alternative suffices, the Court may dismiss the indictment or take other measures.").

simply result in a game of chicken between the executive branch and the judiciary.

C. Shifting the Burden of Proof

Perhaps the simplest solution is to shift the burden of proving the applicability of a policy exclusion from the insurer to the insured. Ordinarily, the insured must only establish a prima facie case for coverage and the insurer bears the burden of proving that a particular loss is excluded under the policy's terms.[103] Reversing the burden—requiring the insured to prove the *in*applicability of a policy exclusion by a preponderance of the evidence—would allow cases to proceed that would otherwise be dismissed on state secrets grounds.[104] The insured's expert would testify fully regarding the evidence underlying their attribution to a nonstate actor. The jury could then evaluate whether the insurer has adequately rebutted the presumption that the perpetrator was a state actor. While this solution requires the least structural reform of those discussed in this Essay, shifting the burden creates a peculiar inconsistency—the presence of an insurance policy is coupled with a presumption of *lack* of coverage. Additionally, merely shifting the burden leads to coverage disputes hinging on the burden, rather than the truth. We would be trading a system in which the *insured* always loses when the insurer asserts the policy exclusion (because the state secrets privilege and subsequent dismissal would lead insurers to have the final word on coverage) to a system in which the *insurer* always loses (because the crucial evidence to rebut the presumption of coverage would be classified).[105] Shifting the burden provides an easily implemented but ultimately unsatisfying solution to address the complex problem of adjudicating cybercoverage disputes involving the hostile-or-warlike-action exclusion.

D. The National Security Court

The creation of a National Security Court (NSC) is another possible approach for addressing coverage disputes arising out of cyberbreaches. For over a decade, scholars, practitioners, and government officials have debated the merits of an NSC in adjudicating terrorism-related matters.[106] The NSC, according to

---

103. *See supra* note 7 and accompanying text.

104. *See supra* notes 56-59; Section III.B.

105. *See supra* notes 56-59; Section III.B.

106. *See, e.g.*, Amos N. Guiora, *Suspected Terrorists: Domestic Terror Courts Are Waiting!*, 156 U. PA. L. REV. PENNUMBRA 357 (2008); John T. Parry, *Managing Suspected Terrorists*, 156 U. PA. L. REV. PENNUMBRA 364 (2008); Harvey Rishikof, *Is It Time for a Federal Terrorist Court?*

its proponents, would avoid burdening ordinary civilian courts with the extraordinary measures necessary to litigate terrorism cases.[107] In a 2007 article, Jack Goldsmith and Neal Katyal suggested that an NSC may also help solve some of the challenges faced in civil cases involving national security issues.[108] The article, however, provided few details on how the court would operate or which civil matters it should try. Former Assistant United States Attorney Andrew McCarthy echoed calls for an NSC in a 2009 working paper, as have other lawyers. [109]

The NSC's jurisdiction could extend to critical questions in cyber-insurance coverage disputes given their nexus to national security. This would be particularly useful in cases involving allegations that state-sponsored or nation-state actors are responsible, for instance those to whom the hostile-or-warlike-action exclusion might apply. Not all cyberbreaches, however, implicate national security concerns. When a breach arises out of ordinary criminal conduct, hearings before the NSC may not be needed. It may be initially unclear whether a case implicates national security issues. However, a transfer procedure could be implemented, allowing cases to be removed from ordinary federal courts to the NSC.[110] Additionally, to protect national security, the court, rather than a jury, could decide all cases. Finally, like the Foreign Intelligence Surveillance Court (FISC), which rules on warrants under the Foreign Intelligence Surveillance Act (FISA), the NSC could issue all decisions under seal.[111]

Terrorists and Prosecutions: Problems, Paradigms, and Paradoxes, 8 SUFFOLK J. TRIAL & APP. ADVOC. 1 (2003); Glenn M. Sulmasy, *The Legal Landscape After* Hamdan: *The Creation of Homeland Security Courts*, 13 NEW ENG. J. INT'L & COMP. L. 1 (2006); Michael B. Mukasey, *Jose Padilla Makes Bad Law*, WALL ST. J. (Aug. 22, 2007, 12:01 AM), https://www.wsj.com/articles/SB118773278963904523 [https://perma.cc/9ZZC-89JS]; Stuart Taylor Jr., *The Case for a National Security Court*, ATLANTIC (Feb. 2007), https://www.theatlantic.com/magazine/archive/2007/02/the-case-for-a-national-security-court/305717 [https://perma.cc/7ZAY-AQ6W]; Andrew C. McCarthy & Alykhan Velshi, *Outsourcing American Law: We Need a National Security Court* (Am. Enterprise Inst., Working Paper No. 156, 2009).

107. *See* STEPHEN DYCUS ET AL., NATIONAL SECURITY LAW 1157-58 (6th ed. 2016).

108. Jack L. Goldsmith & Neal Katyal, *The Terrorists' Court*, N.Y. TIMES (July 11, 2007), https://www.nytimes.com/2007/07/11/opinion/11katyal.html [https://perma.cc/4UVY-45WJ].

109. *See* McCarthy & Velshi, *supra* note 106.

110. The exact nature of the transfer procedure is beyond the scope of this Essay. There are, however, procedures in place for transferring cases between courts. For example, 28 U.S.C. § 1404(a) (2018) allows a district court to transfer a case "to any other district or division where it might have been brought or to any district or division to which all parties have consented." A district court could use this procedure to transfer a cyber breach case to the NSC upon finding it involves national security. If the national security issues are not obvious, the court could conduct a preliminary hearing to hear evidence, in camera or ex parte if needed, on the matter

111. 50 U.S.C. § 1822(a)(3) (2018). Under the USA Freedom Act, the Director of National Intelligence must review every FISC order and opinion to determine whether it "includes a

In implementing the NSC, policy-makers must remain mindful of the larger regulatory framework. At least for publicly traded companies, SEC filings could indirectly reveal a court's decision that a loss is covered under the insured's policy.[112] These filings include insurers' aggregate claims paid for the year. While small payouts may go unnoticed, substantial payouts might raise red flags.

To be sure, the creation of an NSC does not enjoy unanimous support.[113] Much like the FISC, the NSC would operate largely in secret.[114] Thus, the NSC could face similar criticisms regarding a lack of transparency in decision-making.[115] This is a significant criticism of the FISC, whose decisions can grant the government permission to legally infringe on an individual's civil rights. The NSC may suffer the same ills in much of its docket. With respect to insurance disputes, however, these concerns are less significant. Cyberattacks certainly can be important national events. And the perpetrator's true identity may be valuable information to the public. Ultimately, however, the court would merely be deciding a business dispute between two companies. Additionally, without such a court, insureds may be left without a means of accurately adjudicating the coverage dispute. The NSC might offer the best solution for addressing coverage disputes involving cyberbreaches. It provides a comprehensive solution with relatively limited drawbacks.

---

significant construction or interpretation of any provision of law." If so, the order or opinion must be made public "to the greatest extent practicable," though a summary may be released instead to protect national security. 50 U.S.C. § 1872(a) (2018). Thus, while the overwhelming majority of opinions and orders remain sealed, there is a legal provision for unsealing a subset of decisions. To be sure, keeping the NSC's decisions under wraps may be more difficult than the FISC's.

112. *See, e.g.*, *Annual Report 2017*, TRAVELERS INS. (Feb. 15, 2018), http://investor.travelers.com/interactive/newlookandfeel/4055530/travelers2017/download/Travelers_2017AnnualReport.pdf [https://perma.cc/VK9V-YMJG]; *Annual Report 2017*, ZURICH INS. GROUP (Feb. 7, 2018), https://www.zurich.com/_/media/dbe/corporate/docs/financial-reports/2017/annual-report-2017.pdf [https://perma.cc/D59E-U7HD].

113. *See* Steven I. Vladeck, *The Case Against National Security Courts*, 45 WILLAMETTE L. REV. 505 (2009); Constitution Project, *A Critique of "National Security Courts"*, AM. B. ASS'N (June 23, 2008), https://www.americanbar.org/content/dam/aba/migrated/2011_build/law_national_security/critique_ofthe_nat_security_crts_updated_signers.pdf [https://perma.cc/KE3G-2RHT].

114. Only approximately seventy FISC and Foreign Intelligence Surveillance Court of Review opinions have been made public. Laura Donohue, *Georgetown Law's Comprehensive Foreign Intelligence Law Collection*, LAWFARE (June 10, 2019, 2:09 PM), https://www.lawfareblog.com/georgetown-laws-comprehensive-foreign-intelligence-law-collection [https://perma.cc/M5JK-LLNW].

115. *Cf.* Dakota S. Rudesill, *It's Time to Come to Terms with Secret Law: Part I*, JUST SECURITY (July 20, 2016), https://www.justsecurity.org/32120/time-terms-secret-law-part [https://perma.cc/Z5Q4-BAN6].

CONCLUSION

Cyberattacks continue to grow in sophistication and frequency. The cyber-insurance market is growing in response. Many insurance policies, however, contain exclusions for hostile-or-warlike actions perpetrated by a government and its agents. The skirmish between Mondelez and its insurer Zurich highlights the importance of considering the meaning and applicability of this exclusion. Insurers face difficulties when trying to make sure that they provide coverage only for those losses they intended to cover, and that they have taken actuarial account of the insured's premiums. Current procedures are likely to prove inadequate for attributing these attacks and adjudicating coverage disputes. Creating alternative procedures for attributing attacks and handling classified information in the resulting civil cases may allow these disputes to be resolved more effectively. The creation of an NCSB may help alleviate some of the difficulties in attributing cyberattacks by assigning the task to one agency. The agency, however, would not be able to stop attribution disputes and resulting litigation over cyber-insurance coverage.

We must therefore consider jurisprudential solutions for the disputes that do head to the courtroom, such as the expansion of CIPA, shifting the burden of proving the applicability of a policy exclusion, or the creation of an NSC. While all three jurisprudential solutions have drawbacks, an NSC empowered to hear insurance-coverage disputes offers the best avenue for increasing the likelihood that coverage determinations are accurately made in the wake of cyberattacks. Future scholarship should consider details regarding the structure of the court, appropriate means for staffing the court,[116] and the procedures for transferring cases. These issues and their solutions will continue to grow in importance as the number of cyberattack victims grows and the victims turn to their insureds to indemnify the losses.

Adam Shniderman is a member of the University of Michigan Law School, class of 2020. He holds a Ph.D. in Criminology, Law, and Society from the University of California, Irvine and a B.A. in Law, Jurisprudence, and Social Thought from Amherst College. Prior to law school, he spent three years as a tenure-track Assistant Professor of Criminal Justice. *Thank you to Professor Kyle Logue for his thoughtful comments on prior drafts of this Essay and to the* Yale Law Journal *editors who have worked on this piece.*

---

116. One staffing question, for instance, is whether to appoint Article I judges or rely on rotating Article III judges as the FISA court does. *See About the Foreign Intelligence Surveillance Court*, U.S. FOREIGN INTELLIGENCE SURVEILLANCE CT., https://www.fisc.uscourts.gov/about-foreign-intelligence-surveillance-court [https://perma.cc/B4E9-TQ8E].