INSURANCE POLICIES AND THE ATTRIBUTION OF CYBER OPERATIONS UNDER INTERNATIONAL LAW: A COMMENTARY

ISABELLA BRUNNER*

The increasing prevalence of cyber operations, conducted by both State and non-State actors, has caused significant monetary damage to companies and governments worldwide. For example, the 2017 "NotPetya" cyber operation allegedly caused financial damage of at least $10 billion dollars.[1] While insurers have been paying out to affected companies (depending on the policy adopted between insurer and company), many insurers increasingly refuse to cover costs incurred by cyber operations. In particular, two cases related to the NotPetya cyber operation were brought to court by companies Merck and Mondelez, respectively, because the insurer refused to pay, arguing that NotPetya constituted a "war or hostile act." Moreover, most recently, Lloyd's of London, an insurance company, prominently stated that it will

* LL.M. in International Legal Studies, Fulbright Scholar, and Dean's Graduate Award Recipient at New York University School of Law. Ph.D. candidate in International Law at University of Vienna. I am grateful for the editorial assistance of Alex Mason Pazmiño, Colton Jackson, and Keian Razipour, and the helpful comments of Valentin Weber on earlier drafts. Any and all errors are my own.

1. Josephine Wolff, *How the NotPetya Attack is Reshaping Cyber Insurance*, BROOKINGS TECHSTREAM (Dec. 1, 2021), https://www.brookings.edu/techstream/how-the-notpetya-attack-is-reshaping-cyber-insurance/.

no longer cover "state-backed cyber-attacks" with a significant effect.[2]

Evidently, insurers are looking for ways to avoid paying for damages amounting to millions or even billions for unprecedented cyber operations. However, the recent moves by insurance companies raise interesting questions as to the relevance of international law in these discussions. For example, much of the wording in these policies refers to conduct traditionally reserved for States and regulated under international law.

By setting new guidelines for excluding State-backed cyber operations and putting forward criteria that designate when conduct is attributable to a State, Lloyd's of London is arguably dipping its toes into a field traditionally reserved for States. While this has been the case in the traditional context as well—such as with traditional war exclusion clauses in insurance policies—the cyber context leaves open further unresolved questions, in particular because of the significant challenges of attributing a cyber operation to a State due to vast possibilities of staying anonymous when conducting such operations. Thus, one of these questions is what the relationship between cyber insurance policies and the rules of attribution under international law is and what it should be.

Before addressing this particular question, it is necessary to provide some background information on the NotPetya incident, which initiated this debate due to its significant financial impact; the two cases against insurance companies that arose out of NotPetya; and Lloyd's of London's subsequent policy change. After that, this commentary provides an overview over the relevant attribution rules under international law and the evidentiary rules attached to it, which—this commentary argues—together form the framework for "legal attributions" under international law. In particular, this commentary addresses the (strict) rules of attribution and how "political attributions" do not meet the

2. *See Market Bulletin: State-Backed Cyber Attack Exclusions*, LLOYD'S OF LONDON (Aug. 16, 2022), https://assets.lloyds.com/media/35926dc8-c885-497b-aed8-6d2f87c1415d/Y5381%20Market%20Bulletin%20-%20Cyber-attack%20exclusions.pdf [hereinafter Lloyd's of London Market Bulletin 2022] (setting out details of required exclusions for State-backed cyber attacks in insurance policies).

standard of "legal attributions," as they tend to not meet necessary evidentiary standards. Then, this commentary examines how insurance companies reach into the area of international law, by addressing —through their policies— "state-backed cyber attacks" and how this relates to the attribution of cyber operations under international law. This commentary concludes by discussing the forthcomings and pitfalls of applying "international law language" to insurance cases and litigations that are not subject to international law and discussing the implications that precedents in the insurance industry may have on international adjudication pertaining to the attribution of cyber operations to States.

I. NotPetya, Merck, Mondelez and Lloyd's of London – an Overview

A. *NotPetya*

NotPetya was a cyber operation that was allegedly launched by the Russian Federation against Ukraine in June 2017.[3] While Ukraine was allegedly the main target, the malware spread worldwide, causing financial damages in the amount of at least $10 billion.[4] Australia, Canada, Denmark, Japan, New Zealand, the United States, the United Kingdom, and Ukraine attributed the incident to the Russian Federation in February 2018.[5] The European Union condemned the

3. *See* Andy Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, Wired.com (Aug. 22, 2018), https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ (for a history and description of the NotPetya attack).

4. Elizabeth Braw, *We're in an Age of Cyber-Warfare – and Businesses are About to be More Exposed Than Ever*, Prospect Magazine (Sep. 1, 2022), https://www.prospectmagazine.co.uk/science-and-technology/were-in-an-age-of-cyber-warfare-and-businesses-are-about-to-be-more-exposed-than-ever.

5. Australian Minister for Law Enforcement and Cyber Security, *Australian Government Attribution of the "NotPetya" Cyber Incident to Russia* (Feb. 16, 2018), https://www.dfat.gov.au/sites/default/files/australia-attributes-notpetya-malware-to-russia.pdf; Government of Canada, *CSE Statement on the NotPetya Malware* (March 24, 2021), https://cse-cst.gc.ca/en/information-and-resources/news/cse-statement-notpetya-malware; *Claus Hjort: Rusland Stod Bag Cyberangreb Mod Mærsk,* Berlingske (Feb. 15, 2018), https://www.berlingske.dk/virksomheder/claus-hjort-rusland-stod-bag-cyberangreb-mod-maersk; Florian Egloff, *Public Attribution of Cyber Intrusions*, 6 J. of Cybersecurity 1, 8 (2020); New Zealand Government, *New Zealand Joins International Condemnation of NotPetya Cyber-Attack*, New Zealand Gov't Comm. Se-

NotPetya operation on April 16, 2018, without explicitly naming Russia.[6] On July 30, 2020, however, it imposed sanctions against the unit within the Russian GRU—a military intelligence agency allegedly responsible for the act.[7]

NotPetya exemplifies the potential damages large-scale cyber operations can cause. It is, however, far from an isolated incident. Many cyber operations have caused large financial damages, including the SolarWinds cyber operation against countless U.S. companies, discovered in December 2020, which allegedly cost the companies an average of $12 million,[8] or the ransomware attack against the U.S. Colonial Pipeline in May 2021, which allegedly led toColonial Pipeline paying $5 million in Bitcoin to retrieve data.[9] In May 2022, Costa Rica announced a nation-wide state of emergency caused by a cyber ransomware attack allegedly undertaken by a cybercriminal group—with some loose ties to the Russian government[10]—

---

curity Bureau (Feb. 16, 2018), https://www.gcsb.govt.nz/news/new-zealand-joins-international-condemnation-of-notpetya-cyber-attack/; *Statement from the Press Secretary*, The White House (Feb. 15, 2018), https://trumpwhitehouse.archives.gov/briefings-statements/statement-press-secretary-25/ [hereinafter White House Statement 2018]; *Russian Military "Almost Certainly" Responsible for Destructive 2017 Cyber Attack,* U.K. Nat'l Cyber Security Centre (Feb. 14, 2018), https://www.ncsc.gov.uk/news/russian-military-almost-certainly-responsible-destructive-2017-cyber-attack [hereinafter UK NCSC Statement 2018].

6. *Response to Malicious Cyber Activities: Council Adopts Conclusions,* Council of the E.U. (April 16, 2018), https://www.consilium.europa.eu/en/press/press-releases/2018/04/16/malicious-cyber-activities-council-adopts-conclusions/.

7. *See* Council Decision (CFSP) 2019/797, 2019 O.J. (L 1291) 13; Council Regulation (EU) 2019/796, 2019 O.J. (L 1291) 1.

8. *2021 Cybersecurity Impact Report: Amid Escalating Attacks, Organizations Explore New Strategies*, IronNet (2021), https://www.ironnet.com/hubfs/IronNet-2021-Cybersecurity-Impact-Report-June2021.pdf?hsLang=en&submissionGuid=39c8446a-6789-41e5-8652-a7dd61b8af94.

9. Ivan Nechepurenko, *Russia Says It Shut Down Notorious Hacker Group at U.S. Request*, N.Y. Times (Jan. 14, 2022), https://www.nytimes.com/2022/01/14/world/europe/revil-ransomware-russia-arrests.html [hereinafter Nechepurenko].

10. *See* Matt Burgess, *Leaked Ransomware Docs Show Conti Helping Putin From the Shadows*, Wired (March 10, 2022), https://www.wired.com/story/conti-ransomware-russia/ [hereinafter Burgess].

with financial losses ranging from $38 million per day to up to $125 million over 48 hours.[11]

Moreover, there are no signs that cyber operations are in any way declining. More robust cybersecurity practices may help to reduce the damages caused by such operations, but in the meantime, insurance policies have helped to at least cover parts of the financial losses. Increasingly, however, insurers are charging higher premiums and lowering their coverage for such incidents.[12] In the *Merck* and *Mondelez* cases, insurers even started refusing to pay out parts of the insurance altogether.

B. *Merck and Mondelez*

After the NotPetya cyber operation had hit computer systems of Merck, a multinational pharmaceutical company, Merck had asked its insurers to pay out insurance to cover any "loss or damage resulting from destruction or corruption of computer data and software."[13] The insurers, however, argued that in the NotPetya instance, a "hostile or warlike act" exclusion applied. According to such exclusion, "[l]oss or damage caused by hostile or warlike action in time of peace or war, . . . by any government or sovereign power . . . or by an agent of such government, power, authority or forces" would not be covered by the insurance policy.[14]

In the Statement of Facts in *Merck v. Ace,* the Superior Court of New Jersey noted that the parties disputed "the issue of whether the facts show conclusively . . . that the malware, called 'NotPetya,' was an instrument of the Russian government."[15] While the insurer argued that there was overwhelm-

---

11. Costa Rica Declares National Emergency Amid Ransomware Attacks, THE GUARDIAN (May 12, 2022), https://www.theguardian.com/world/2022/may/12/costa-rica-national-emergency-ransomware-attacks; Matt Burgess, *Conti's Attack Against Costa Rica Sparks a New Ransomware Era*, WIRED (June 12, 2022), https://www.wired.com/story/costa-rica-ransomware-conti/.

12. *See* Tom Uren, *Act of God or Act of Hacker, It's All the Same to Us*, SERIOUSLY RISKY BUSINESS (August 25, 2022), https://srslyriskybiz.substack.com/p/act-of-god-or-act-of-hacker-its-all?utm_source=EMail&publication_id=34083&post_id=70230533 (providing an overview of developments in the cyber insurance industry).

13. Civil Action Order at 2, Merck & Co., Inc., and Int'l Indemnity, Ltd. v. Ace American Insurance Co., et al., No. UNN-L-2682-18 (N.J. Super. Ct. Law Div, Dec. 6, 2021) [hereinafter Merck v. Ace].

14. *Id.* at 3.

15. *Id.*

ing evidence of Russian State origin, Merck argued that "there [were] significant facts which show it was not an official State action, but rather . . . a form of ransomware."[16] In the end, the court did not focus on this evidentiary question, but rather found that the "hostile or warlike acts exclusion" clause did not apply in this case because the insurer had failed to clarify that cyber operations could fall under this clause. Hence, Merck could reasonably assume that such an exclusion clause would only apply to "traditional forms of warfare."[17] As a result, Merck prevailed, and the insurer was required to pay the requested amount.

Mondelez, a multinational food corporation was also heavily affected by the NotPetya cyber incident. According to the Financial Times, 1,700 of Mondelez' servers and 24,000 laptops were rendered "permanently dysfunctional" by NotPetya.[18] In January 2019, Mondelez filed a lawsuit against its insurer, Zurich Insurance, because Zurich refused to pay out insurance in the amount of $100 million.[19] Mondelez argued that the NotPetya cyber incident was covered by the insurance with Zurich. Zurich's counterargument—similar to that of the insurer in the Merck case—was that NotPetya constitutes a war or hostile act which would be excluded from insurance.[20] The case was pending before an Illinois State Court for a long time, before the parties finally reached a settlement at the end of October 2022.[21]

C. Lloyd's of London's *exclusion of "State-backed cyber attacks"*

Likely because of these recent court developments, on August 16, 2022, Lloyd's of London published a market bulle-

16. *Id.*

17. *Id.* at 11.

18. Oliver Ralph and Robert Armstrong, *Mondelez Sues Zurich in Test for Cyber Hack Insurance*, FINANCIAL TIMES (Jan. 9, 2019), https://www.ft.com/content/8db7251c-1411-11e9-a581-4ff78404524e [hereinafter Ralph and Armstrong 2019].

19. *Id.*

20. Mondelez Int'l, Inc. v. Zurich Am. Ins. Co., No. 2018L011008, 2018 WL 4941760, at 3, ¶ 15 (Ill. Cir. Ct. Oct. 10, 2018).

21. Alexander Martin, *Mondelez and Zurich Reach Settlement in NotPetya Cyberattack Insurance Suit*, THE RECORD (Oct. 31, 2022), https://therecord.media/mondelez-and-zurich-reach-settlement-in-notpetya-cyberattack-insurance-suit/. The details of the settlement are unknown at the time of writing.

tin for its underwriters to clarify that Lloyd's of London will no longer cover insurance for "State-backed cyber attacks."[22] This policy will be effective starting from March 31, 2023.[23] As a requirement of exclusion, such "State-backed cyber attacks" must either "significantly impair the ability of a state to function" or "significantly impair the security capabilities of a state."[24] While the bulletin itself does not specify how to attribute a cyber "attack" to a State, Lloyd's of London provides further guidance in its model exclusion clauses, which—while being "purely illustrative"[25]—could be used by its underwriters and insured companies.

In particular, all four model clauses note that a primary—while not exclusive—factor for considering an operation as "State-backed" should be whether the State affected by the operation has attributed the incident to a State "or those acting on its behalf."[26] Until the State has attributed the incident, "the insurer may rely upon an inference which is objectively reasonable as to attribution of the cyber operation to another state or those acting on its behalf."[27] If the State chooses not to attribute, it may be up to the insurer to prove the attribution with "such other evidence as is available."[28] What such other evidence may be is not mentioned.

In any event, Lloyd's of London's bulletin notes that the exclusion clause must "set out a robust basis by which the parties agree on how any State-backed cyberattack will be attributed to one or more states."[29] This commentary argues that, merely basing an attribution on a government's political attribution statement should not be considered a "robust basis."

---

22. Lloyd's of London Market Bulletin 2022, *supra* note 2, at 2.

23. *Id.*

24. *Id.*

25. *Cyber War and Cyber Operation Exclusion Clauses*, LMA LLOYDS (Nov. 25, 2021), https://www.lmalloyds.com/LMA/News/LMA_bulletins/LMA_Bulletins/LMA21-042-PD.aspx.

26. *Lloyd's of London Model Exclusion Clauses No. 1-4*, LMA LLOYDS (Nov. 25, 2021), https://www.lmalloyds.com/LMA/News/LMA_bulletins/LMA_Bulletins/LMA21-042-PD.aspx.

27. *Lloyd's of London Model Exclusion Clause No. 1*, LMA LLOYDS (Nov. 25, 2021), https://www.lmalloyds.com/LMA/News/LMA_bulletins/LMA_Bulletins/LMA21-042-PD.aspx.

28. *Id.*

29. Lloyd's of London Market Bulletin 2022, *supra* note 2, at 2.

II. Attribution of Cyber Operations to a State under International Law

This commentary does not question that the interpretation of (cyber) insurance policies is regulated under private law. Thus, public international law, and in particular the rules of attribution under the International Law Commission Articles on the Responsibility of States for Internationally Wrongful Acts (ILC Articles)[30] and evidentiary rules related to attribution, is not directly applicable to disputes arising between private parties in a national court proceeding. However, given the particular uncertainty regarding the questions of attribution and how they are applicable to cyber operations, national court judgments could potentially be considered as persuasive authority in future judgments rendered by the International Court of Justice or another international tribunal having jurisdiction over the attribution of cyber operations to the State. At the same time, the rules of attribution and accompanying evidentiary rules under international law may also be indicative for national courts in their assessment whether a cyber operation is attributable to a State. That may be the case particularly if the national court judgment is not only based on a "political" attribution statement made by a State.

As noted above, together with evidentiary rules, the ILC Articles form the framework for "legal attribution" of an internationally wrongful act to a State.[31] The ILC Articles set out which conduct is attributable to a State under its Articles 4-11. For the purposes of this commentary, Articles 4 and 8, related to acts conducted by a State organ and acts conducted by a non-State actor, respectively, are the most relevant to assess when a state may be held responsible. Cyber operations tend to be conducted either directly by a cyber unit of a specific State—e.g. the Russian GRU or the Chinese Ministry of State Security—or by non-State actors with which States have an "es-

30. *Draft Articles on Responsibility of States for Internationally Wrongful Acts*, Int'l L. Comm' n, Supplement No. 10 (A/56/10) (Nov. 2001), https://www.refworld.org/docid/3ddb8f804.html [hereinafter ILC Articles].

31. *See id* art 2. It is important to note that this article does not address whether any of the mentioned cyber operations constitute an internationally wrongful act, i.e., a breach of an international obligation of a State, which is necessary—next to attribution—in order to establish State responsibility under international law.

tablished and systematic relationship"[32]—e.g., Russian cybercriminal groups like Cozy Bear or the group behind the REvil ransomware.[33] Regarding the latter, ILC Article 8 foresees that the conduct needs to be either directed, instructed, or controlled by the State. There is, however, a lively academic debate as to which threshold of control needs to be exercised by the State in order to attribute the conduct to the State. Some authors, for example, have called for lowering the threshold of 'effective control'—as determined by the ICJ in the *Nicaragua* case and reaffirmed in the *Bosnian Genocide* case[34]—to 'overall control'—as determined by the ICTY in *Tadic*[35]—or even 'virtual control,' which, essentially, is a proposal to shift the burden of proving control to the State having allegedly provided financial or other assistance to a private group.[36] States, on the other hand, have not been very specific regarding the necessary threshold, although Brazil, the Netherlands, and Norway have noted in their position on international law applicable to cyberspace that the necessary threshold remains 'effective control'—the most stringent threshold of control.[37]

Next to the ILC Articles, it is argued that additionally, evidentiary rules exist that determine the sufficiency of evidence

---

32. Nechepurenko 2022, *supra* note 9.

33. *See Adversary: Cozy Bear,* CROWDSTRIKE, https://adversary.crowdstrike.com/en-US/adversary/cozy-bear/ (CrowdStrike, a cybersecurity company, assessing Cozy Bear as "likely to be acting on behalf of the Foreign Intelligence Service of the Russian Federation"); *see* Jonathan Vanian, *Everything to Know About REvil, the Group Behind a Big Ransomware Spree*, FORTUNE (July 7, 2021), https://fortune.com/2021/07/07/what-is-revil-ransomware-attack-kaseya/.

34. *Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.)*, Merits, Judgment, 1986 I.C.J.14, ¶ 115 (June 27); *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. and Montenegro)*, Merits, Judgment, 2007 I.C.J., ¶ 401 (Feb. 26).

35. Prosecutor v. Tadic, Case No. IT-94-1-I, Judgement on Appeal, ¶ 122, 131 (Int'l Crim. Trib. for the Former Yugoslavia Jul. 15, 1995).

36. On lowering the standard of control, see, *inter alia*, Scott J Shackelford, *From Nuclear War to Net War: Analogizing Cyberattacks in International Law*, 27 BERKELEY J. OF INT'L L. 191, 233ff (2009); David J Ryan et al, *International Cyberlaw: A Normative Approach*, 42 GEORGETOWN J. OF INT'L L. 1161, 1187f (2011); *see* Peter Margulies, *Sovereignty and Cyberattacks: Technology's Challenge to the Law of State Responsibility*, 14 MELBOURNE J. OF INT'L L. 496 (2013) (explaining the argument of lowering to "virtual control").

37. *See Attribution,* CyberLaw Toolkit (Sep. 12, 2022), https://cyberlaw.ccdcoe.org/wiki/Attribution for a collection of national positions on attribution.

necessary for legally attributing an act to a State. Arguably, legal attributions would have to be established with "clear and convincing evidence," and inferences of fact may leave "no room for reasonable doubt."[38] In that context, both for attributing conduct by a State organ or non-State actor, there are considerable evidentiary challenges. While some claim that attribution of cyber operations is not impossible,[39] providing the necessary proof reaching the "clear and convincing evidence" threshold still remains difficult as there are many ways to obscure the origins of an attack—e.g. through false flag operations, IP spoofing, etc.[40] With respect to proving instruction, direction, or control of a non-State group for attributing to a State, the threshold of control—be it either "effective" or "overall" control—provides further evidentiary difficulties. Also, while it might be possible to attribute an act to a specific location, it is much more difficult to establish a concrete link to a human being linked to a State,[41] be it a State organ or a non-State actor acting under the instructions, directions, or control of a State.

So far, it seems that States have been reluctant to refer specifically to the ILC Articles or any evidentiary rules in particular, when condemning a State for conducting a cyber operation. Rather, they have stuck to so-called "political attributions," which have gained more and more significance in international relations.[42] "Political attributions," as the name says,

---

38. *Corfu Channel (U.K. v. Alb.)*, Merits, Judgment, 1949 I.C.J. Rep, at 18 (Apr. 9); Isabella Brunner, Marija Dobric and Verena Pirker, *Proving a State's Involvement in a Cyber-Attack: Evidentiary Standards Before the ICJ*, 25 FINNISH Y.B. OF INT'L L. 75, 97 (2019).

39. *See, inter alia*, *A Guide to Cyber Attribution,* OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE (Sep. 14, 2018), https://dl.icdst.org/pdfs/files3/db004a6f55f96c056a23fc4efc6a23ac.pdf (arguing that attribution is often possible, if difficult, and explaining the conditions necessary for attribution).

40. *See* MARCO ROSCINI, CYBER OPERATIONS AND THE USE OF FORCE IN INTERNATIONAL LAW 251 (Oxford Univ. Press, 2015); Florian Skopik and Timea Pahi, *Under False Flag: Using Technical Artifacts for Cyber Attack Attribution*, 3 CYBERSECURITY 1 (2020) for some overview of these methods.

41. Herbert Lin, *Attribution of Malicious Cyber Incidents: From Soup to Nuts,* HOOVER WORKING GROUP ON NAT'L SECURITY, TECH., AND L., AEGIS PAPER SERIES NO. 1607, 8 (Sept. 26, 2016).

42. *Cf.* Isabella Brunner, *The Prospects for an International Attribution Mechanism for Cyber Operations: An Analysis of Existing Approaches*, SSRN (July 3, 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3986297 (dis-

are attributions made at the political, rather than legal, level and—despite States' attempts to appear as objectively as possible—they are nevertheless *politically charged*. They serve to publicly condemn a cyber action conducted by a specific State, usually without providing a legal source or much public evidence to support the assumption.[43]

However, "unlike courts, different intelligence services might offer competing assessments of the same incidents."[44] These assessments are—as noted above—usually not shared with the public, but the public statements may also differ in terms of how much information States provide as to their confidence in the attribution. As an example, while the United States does not elaborate on its certainty that Russia was behind the NotPetya cyber operation, the United Kingdom assessed that Russia was "*almost* certainly" responsible. At the same time, those that have been considered the "originators" of the wrongful cyber operations—such as Russia in the case of NotPetya—simply rejected such statements by denying all of the claims made therein.[45] Although eventually not addressed by the U.S. court in the *Merck* case, Merck also challenged the

---

cussing the possibility of an independent international attribution mechanism).

43. It might be important to note that this analysis does not include criminal indictments made by States for cybercriminal acts, such as in the case of United States v. Wang Dong et al, No. 14-118 (W. D. Penn., 2014) https://www.justice.gov/iso/opa/resources/5122014519132358461949.pdf; on the argument that this could be considered an attribution, see Chimène I Keitner, *Attribution by Indictment*, 113 AJIL UNBOUND 207 (2019) [hereinafter Keitner 2019]; also note that some States are of the opinion that they are not legally obligated to provide evidence when conducting an attribution. For more on this view *see*, *inter alia*, Former U.K. Attorney General Jeremy Wright, *Cyber and International Law in the 21st Century* (May 23, 2018), https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century (stating " there is no legal obligation requiring a state to publicly disclose the underlying information on which its decision to attribute hostile activity is based, or to publicly attribute hostile cyber activity that it has suffered in all circumstances").

44. Jon Bateman, *War, Terrorism, and Catastrophe in Cyber Insurance: Understanding and Reforming Exclusions*, CARNEGIE ENDOWMENT FOR INT'L PEACE, 13 (Oct. 1, 2020), https://www.jstor.org/stable/resrep26177.5?seq=2#metadata_info_tab_contents.

45. *See* Ralph and Armstrong 2019, *supra* note 18, for an example of such a denial on the part of Russia. For another example, China, who said that the US was making "groundless accusations" against China for a hack against the Office of Personnel Management, see Milton Mueller et al, *Cyber Attribu-*

insurer's argument that NotPetya is state-backed by pointing to "significant facts."[46] Some experts have termed this dilemma of the originator States being able to deflect responsibility due to evidentiary gaps as "plausible deniability."[47] Thus, such political attribution statements could not be considered "legal attribution" in the sense of international law, nor—in order to ensure consistency—should they be considered a sufficient basis for national court judgments considering the attribution of cyber operations to a State.

This, however, is what Lloyd's of London attempts to achieve with its new insurance policy. In particular, Lloyd's of London is trying to link a State's political attribution statement, which States regularly stress is not a legal attribution in itself, to its own legal obligation to discharge proof that a cyber operation is "State-backed," thus excluding coverage for such an attack. Lloyd's of London's model clauses—as a preliminary step—only require that a State has attributed the incident itself, without providing any additional requirements as to evidentiary standards or rules. This would enable insurers to exclude insurance on the basis of insufficiently proven "political attribution" statements. If accepted by a court, such conclusions would rely on complete trust in a government's attribution assessment without any measure of oversight or transparency.

It would be better, therefore, if the insurer was obliged to provide additional evidence, in particular, in a court proceeding, such as through reports of cybersecurity companies containing concrete evidence or its own investigations, to back up the claims of the State. A national court judgment, if not solely based on vague attribution statements made by States but which instead is based on concrete and sufficient evidence, may be persuasive authority also for international courts and tribunals to establish attribution in a cyber case. The International Court of Justice, for example, may rely on national judi-

---

tion: Can a New Institution Achieve Transnational Credibility?, 4 THE CYBER DEF. REV. 107, 107 (2019).

46. Merck v. Ace, *supra* note 13, at 3.

47. *See* CLEMENT GUITTON, INSIDE THE ENEMY'S COMPUTER: IDENTIFYING CYBER ATTACKERS 163-182 (Oxford Univ. Press 2017) (providing an in-depth discussion of attribution and its challenges).

cial decisions as "subsidiary means for the determination of rules of law."[48]

III. Conclusion

Cyber insurance policies may, at first glance, not be particularly related to international law. However, the increasing cross-border nature of cyber operations and the damages they can cause worldwide, force insurers to think globally. International law has elaborate rules about the attribution of cyber operations to a State and applying these rules to ascertain the question whether a cyber operation is "State-backed" may contribute to the discussion taking place in the insurance industry.

Linking the discussions taking place in the insurance industry and international law discussions could be beneficial to both fields where they both must deal with the growing impact of transborder cyber operations. Thus, it will remain crucial to observe both insurance policies and developments in international law to reach conclusions that do not contradict each other. That said, cyber insurance cases adjudicated at national levels could contribute to establishing more concrete assessments regarding the attribution of cyber operations to a State. Thus, if cyber insurance companies try to base the attribution solely on political attribution statements made by States, they are not contributing sufficiently. Also, if, in the future, national court judgments—by endorsing such conduct—reinforce the attribution made by a State without seeing any further evidence, they contribute to setting in stone that specific attribution statement, thereby further promoting the opaqueness that is prevalent in the "political attribution" process. Thus, it should not be acceptable for insurance companies to discharge their burden of proof in such a way.

It is, of course, understandable that cyber insurance companies would like to exclude as many cyber operations as possible from their coverage. However, sufficient evidence should still be required from insurance companies to discharge their burden of proof. If national court judgments thus take into consideration more evidence than just the political attribution

48. Statute of the International Court of Justice, art 38, ¶1d, June 26, 1945, 59 Stat. 1055.

statements, their judgment may be a valuable contribution that could be referred to for the international settlement of attribution disputes between States regarding cyber operations, potentially negotiated in the future.