Cyberattacks: a look at evidentiary thresholds in International Law

Sharngan Aravindakshan

Published online: 17 August 2020
© The Indian Society of International Law 2020

Abstract This paper notes the increasing prevalence of cyberattacks on the international plane and identifies the shortcomings of “public attribution” or “naming-and-shaming”, the tool currently being used by nation states to publicly call out perpetrator-states (including non-state actors) to both punish as well as deter future cyberattacks. The paper points to a need for legally proving attribution in international law as a pre-requisite to receiving any form of redressal or reparations. The paper then examines the current standards and methods of proof in international law and attempts to cull out the nature and amount of evidence required for a state to prove responsibility for a cyberattack in an international legal forum. It concludes that circumstantial evidence is currently the most viable way of proving state responsibility for a cyber operation including cyberattacks and then contextually examines this in the backdrop of the recent malicious cyber incident at India’s nuclear power plant in Kudankulam.

Keywords Cyberattacks · Evidentiary thresholds · International law · Kudankulam

For a while now, scholarly discussions on cyber-attacks have centered around the challenges in attributing any cyber-attack to a nation-state. This is with good reason and no one explains these reasons better than Joel Brenner who observed that “*the Internet is one big masquerade ball. You can hide behind aliases, you can hide behind proxy servers, and you can*

Sharngan Aravindakshan (✉)
Programme Officer, Centre for Communication Governance at National Law University, New Delhi,
India
e-mail: sharngan.aravindakshan@gmail.com

*surreptitiously enslave other computers without their owners' knowledge—and then use their computers to do your dirty work.”*¹

Cyberspace presents a vast array of tools for concealment and disguise. Today, any person can impersonate another computing system (IP spoofing)², anonymize communication through layers of encryption (onion routing)³ and even prevent reverse engineering and deliver untraceable code (obfuscating log files)⁴. These are merely a few techniques among several that enable actors to commit malicious cyber acts with impunity, including nation states.

However, while these issues do make it difficult for public attribution, i.e., a government publicly calling out the perpetrator-state, they present an even larger challenge to the victim state legally *proving* its claims in an international judicial forum. After all, the next step to identifying the perpetrator is claiming remedies and this can only be done once the victim State is able to prove its claims in accordance with evidentiary standards in international law.

Given that states now accept that international law applies to cyberspace⁵, this article first discusses the limitations in public attribution and highlights the need for using legal fora for redressal in cases involving cyber-attacks. This is followed by an examination of the existing requirements and treatment of evidence in international law for international wrongs and teases out the evidentiary thresholds that states will be required to meet to show an international wrong in cyberspace. The article concludes that while it is likely that international judicial forums will not relax standards of proof to accommodate the obvious cyber-challenges, circumstantial evidence is available as a potentially viable route to prove a violation. Since state to state disputes have been more commonly addressed in the International Court of Justice (“**ICJ / Court**”), this article will rely on the standards used by the ICJ, while also pointing out a few decisions by other international judicial forums as well.

¹ Joel Brenner, *America The Vulnerable: Inside The New Threat Matrix Of Digital Espionage, Crime, And Warfare* (Penguin Press 2011) 32.

² Internet Society, ‘Addressing the Challenge of IP Spoofing’ (2015).

³ See generally Michael G Reed, Paul F Syverson and David M Goldschlag, ‘Anonymous Connections and Onion Routing’ (1998) 16 IEEE Journal on Selected Areas in Communications 482.

⁴ See generally Sebastian Schrittwieser and Stefan Katzenbeisser, ‘Code Obfuscation against Static and Dynamic Reverse Engineering’ in Tomáš Filler and others (eds), *Information Hiding*, vol 6958.

⁵ Cyrus Jabbari, ‘The Application of International Law in Cyberspace: State of Play’ (Office of Disarmament Affairs, United Nations, 25 October 2018).

To be clear, the article primarily deals with *standards of proof* and *methods of proof*, both of which must be distinguished from *rules of attribution* in international law. While the standard of proof deals with the *quantum* of evidence required to prove a claim, rules of attribution deal with the *level of control* exercised by the State over a non-state actor that caused the violation.⁶ These rules of attribution primarily find their source in Article 8 of the Articles of Responsibility of States in Internationally Wrongful Acts⁷ (“**Articles of State Responsibility**”) as well as the extremely strict “effective control” test formulated by the ICJ in *Nicaragua v. United States* (“**Nicaragua**”) and the slightly lower standard of “overall control” formulated by the International Criminal Tribunal for the former Yugoslavia in *Prosecutor v. Tadic* (“**Tadic**”). In the cyber domain, new tests are being proposed such as the “control and capabilities” test which is supposedly based on recent state practice in public attribution of cyber-attacks and is one that has an even lower threshold than the overall control test.⁸ While a discussion on these evolving tests is certainly important in the cyber domain, it is worthwhile to point out that these tests of attribution should not be conflated with the standards of proof that states’ evidence must meet to prove their claims.

1 Limitations of public attribution and the need for legal attribution

Public attribution, the practice of calling out perpetrators of malicious cyber activities, is currently among the few tools of deterrence available in cyberspace. While recent times have seen several private entities with technical expertise such as Mandiant⁹ and CrowdStrike¹⁰ enter the fray by not only investigating and tracing the malicious activity to the

⁶ Marco Roscini, ‘Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations’ (2015) 50 Texas International Law Journal 233 <https://westminsterresearch.westminster.ac.uk/download/12a3ed1c482904ffa3bee825eb850cfafe06376ffdbba4d839c579d48e998f3/397095/Roscini_TILJ_2015.pdf> accessed 11 February 2020.

⁷ ‘Report of the International Law Commission on the Work of Its Fifty-Third Session, Official Records of the General Assembly, Fifty-Sixth Session’ (2001) UN Doc A/56/10.

⁸ Peter Z Stockburger, ‘Control and Capabilities Test: Toward a New Lex Specialis Governing State Responsibility for Third Party Cyber Incidents’ (NATO CCD COE Publications 2017).

⁹ ‘APT1: Exposing One of China’s Cyber Espionage Units’ (Mandiant 2013) <<https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf>> accessed 11 February 2020.

¹⁰ Nathaniel Hartley, ‘Hat-Tribution to PLA Unit 61486’, CROWDSTRIKE Blog, June 9, 2014, [2] <<https://www.crowdstrike.com/blog/hat-tribution-pla-unit-61486/>>.

perpetrators, but also publicly reporting details of their investigations, this discussion will be limited to instances of public attribution by governments. Public attribution by governments largely consists of statements issued by officials with various levels of formality.¹¹ It is perceived as having several benefits including exposing errant states¹² and driving vulnerable targets to providers to bolster their networks¹³, besides calling public attention to malicious activity in cyberspace. It has particular use in forcing states to draw “red lines” on norms and violations in cyberspace, thereby also contributing to the growth of much needed *opinio juris* in cyberspace.

However, a state that has been victim to a cyber-attack has to also be able to resort to legal remedies since the benefits of public attribution, though important, are still limited.¹⁴ While the exercise of naming and shaming can contribute to *opinio juris*, the repeated involvement of only a handful of states willing to engage in public attribution as well as the lack of any real costs or measures being imposed on the accused state besides the naming and shaming, limits its efficacy as a tool to deter future cyber malicious activity in the international community.¹⁵

Pursuing legal remedies in an international legal forum, on the other hand, can result in tangible benefits such as injunctions and reparations as well as serve as strong reminders to states that cyber mal-activities have real consequences.

Further, judicial determinations in international legal fora ordinarily result from a rigorous process that grants them legitimacy and renders them trustworthy, which can be hard to achieve through public attribution in its present form, chiefly consisting of one-sided accusations by the victim state, often with vocal support from its allies, followed by dismissive denials by the accused state. For instance, the collective public attribution to Russia by the United States, the United Kingdom and the Netherlands for attempting to hack the Organisation for the Prohibition of Chemical Weapons (OPCW) elicited a dismissive Russian response, terming the joint action as “Western spymania” and

¹¹ John S Davis II and others, ‘Stateless Attribution: Toward International Accountability in Cyberspace’ (RAND Corporation 2017) 21.

¹² Stewart Baker, ‘The Attribution Revolution’, *Foreign Policy*, June 17, 2013, [6] <<https://foreignpolicy.com/2013/06/17/the-attribution-revolution/>>.

¹³ Davis II and others, *supra* note 11.

¹⁴ See generally Anushka Kaushik, ‘Public Attribution and Its Scope and Efficacy as a Policy Tool in Cyberspace’ (2019) 6 ORF Digital Debates CyFy Journal 38.

¹⁵ *Ibid.*

that it was the victim of “yet another stage-managed propaganda campaign”.¹⁶

Also, even though the 2015 Report of the United Nations Group of Governmental Experts (UNGGE) expressly provides that accusations of organizing and implementing wrongful acts brought against States should be substantiated¹⁷, states have expressed contrary views. For instance, Brian Egan, the then Legal Advisor to the State Department in the United States, stated that while states may choose to do so, there exists no international legal obligation to reveal evidence on which attribution is based prior to taking appropriate action.¹⁸ Even in the largest yet exercise of collective attribution in which several countries (the United States, Australia, the United Kingdom and many EU countries including Poland, Estonia, Lithuania, the Czech Republic and Denmark) all named Russia as responsible for the cyber-attacks on Georgia¹⁹, thereby giving the impression that there was a strong basis for the allegations, no evidence was publicly disclosed. Refusal to produce evidence can often be perceived as lack of evidence further exacerbating distrust and undermine confidence in claims of public attribution, thereby negating any beneficial outcomes. Hence, it becomes necessary to look at other ways and means of achieving tangible outcomes in disputes involving cyber-attacks, such as legal redressal. For a state to take legal action against another state in an international legal forum for harm caused to it by a malicious cyber activity, it will necessarily have to meet the required evidentiary standards of proof in international law.

¹⁶ Staff Reporter, ‘West Accuses Russia of Global Cyber-Plots’, BBC News, October 4, 2018, [3–14] <<https://www.bbc.com/news/world-europe-45746837>>. See also Pippa Crerar, Jon Henley and Patrick Wintour, ‘Russia Accused of Cyber-Attack on Chemical Weapons Watchdog’, The Guardian, October 4, 2018, [4] <<https://www.theguardian.com/world/2018/oct/04/netherlands-halted-russian-cyber-attack-on-chemical-weapons-body>>.

¹⁷ ‘Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security’ (2015) U.N. Doc. A/70/174 13 <<https://dig.watch/sites/default/files/UN%20GGE%20Report%202015%20%28A-70-174%29.pdf>>.

¹⁸ Brian Egan, Remarks on International Law and Stability in Cyberspace at Berkeley Law School (10 November 2016) 19 <<https://www.justsecurity.org/wp-content/uploads/2016/11/Brian-J.-Egan-International-Law-and-Stability-in-Cyberspace-Berkeley-Nov-2016.pdf>>.

¹⁹ Marika Kartoza, ‘European Countries Condemn Russia Over Georgia Cyberattack’, First Channel, February 20, 2020, <https://1tv.ge/en/news/european-countries-condemn-russia-over-georgia-cyberattack/>.

2 Standards of proof in international law

The highest standard of evidence in law is posited by domestic criminal law which demands proof beyond *reasonable doubt*, while civil cases in most common law jurisdictions only require proof by a *preponderance of evidence* or *balance of probabilities*, i.e., a more likely than not standard. While some scholars note that the nature of international litigation between states in a forum such as the ICJ is more comparable to civil litigation than criminal,²⁰ the Court has typically refrained from laying down any particular standard of proof in the cases dealt by it, preferring to determine causality and responsibility on a case by case basis.

Portions of the Court's decisions concerning the evidence presented before it shed some light on the prevailing standards of proof in international law considered by it. For instance, in *Bosnia and Herzegovina v. Serbia and Montenegro* ("**Bosnian Genocide case**") in which Bosnia alleged that Serbia contributed to and failed to prevent and punish acts of genocide, the Court stated that "...claims against a State involving charges of exceptional gravity must be proved by evidence that is *fully conclusive*"²¹ indicating that the standard of proof in cases of exceptional gravity such as genocide was that of "fully conclusive" evidence.

However, for cases involving use of force, the Court has used different terminology. For instance, the Court in *Nicaragua* explicitly states that it had to ensure that "the facts on which [the claim of the party appearing] is based [is] supported by *convincing evidence*"²² and that there was "no *clear evidence* of the United States having actually exercised such a degree of control in all fields as to justify treating the contras as acting on its behalf."²³ Again, in *Democratic Republic of Congo Vs Uganda* ("**Armed Activities case**") the Court kept referring to evidence that must be "convincingly established" or terms such as "convincing evidence" or "sufficient and convincing evidence" in the context of proving allegations of use of force.²⁴ So the inference vis-à-vis standards

²⁰ Rudiger Wolfrum (ed), 'International Courts and Tribunals, Evidence', *THE MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW* (2012).

²¹ *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*, Judgment, I.C.J. Reports 2007, at 43 [209].

²² *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, Merits, Judgment, I.C.J. Reports 1986 at 14 [24, 29, 62, 109].

²³ *Ibid.*

²⁴ *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda)*, Judgment, I.C.J. Reports 2005 at 168 [72, 91, 136].

of proof is that for violations of exceptional gravity, “*fully conclusive*” evidence is required and for lesser violations, at least “*clear and convincing*” evidence is required. Both these standards set high evidentiary bars to reach.

Where does this leave cyber-attacks? Given these high evidentiary thresholds, how is any victim-state supposed to prove that the perpetrator state carried out an international wrong in cyberspace, with all its vagaries including concealment and disguising issues?

Ongoing efforts to examine issues in application of international law to cyberspace also do not address these issues. The International Group of Experts (IGE) tasked with creating a Manual on the Law of Cyberwarfare under the aegis of the NATO Cooperative Cyber Defence Centre of Excellence, and whose work resulted in the Tallinn Manual 1.0 and the Tallinn Manual 2.0, also did not discuss the standards and methods of proof in international law applicable for cyber-norm violations, instead leaving them to be “determined by the relevant forum”.²⁵ They were not wrong to do so, given that the constituting instruments of most international courts usually leave it to the court to determine issues of burden and standards of proof as well as rules of evidence on their own.²⁶ However, significantly, the IGE in the Tallinn Manual 1.0 do opine that a cyber-attack originating from a state’s governmental cyber infrastructure, while not sufficient to attribute the cyber-attack to that government, is an indication that the state in question is associated with the operation.²⁷ Even though the Tallinn Manual 1.0 also notes the dangers of spoofing and disclaims that this rule be used to pre-determine evidentiary conclusions as to attribution, if applied by states, it could give rise to a rebuttable presumption that the state from whose governmental cyber infrastructure the attack as launched was involved with the attack.²⁸ If and when accepted by states, this would be an important development since it could significantly ease proving cyber-attacks. However, as the Tallinn Manuals stand currently, they are considered by states as more of a “starting point of a conversation” than an authoritative text.²⁹

²⁵ Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press 2017) 83.

²⁶ Chester Brown, ‘Aspects of Evidence in International Adjudication’ in *A Common Law of International Adjudication* (Oxford University Press 2009) 88.

²⁷ Michael N Schmitt (ed), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press 2013) 39.

²⁸ *Ibid* 39–40.

²⁹ Colonel Gary Corn, ‘Tallinn Manual 2.0 – Advancing the Conversation’, *Just Security*, February 15, 2017, [3] <<https://www.justsecurity.org/37812/tallinn-manual-2-0-advancing-conversation/>>.

In any case, scholars have advised against the lowering of the standard of proof in the cyber-context simply on account of identification and attribution issues.³⁰ As Roscini aptly puts it, the standard of proof exists not to disadvantage the claimant but to protect the respondent against false attribution, an all-too-present danger in the cyber-domain.³¹ But while this cautious approach generally bodes well to prevent states from being framed or mistakenly held responsible, it still does nothing to solve the problem of attribution in the cyber-domain, which is plagued by problems of a general lack of evidence and when it exists, the evidence being controlled by another state's territory. However, as discussed in the next section, one viable route appears to be in the proper accumulation of and use of indirect or circumstantial evidence, currently the main form of evidence available in the cyber-domain.

3 Circumstantial evidence in cyberspace

Evidence is of two types –(i) Direct and (ii) Indirect or Circumstantial. While direct evidence establishes a conclusion, circumstantial evidence is commonly understood as evidence that establishes facts and circumstances from which reasonable inferences can be drawn to reach a conclusion. Today, the nature of digital forensic evidence and other intelligence available post any cyber-attack is circumstantial inasmuch as it only gives rise to inferences that can together lead to a conclusion. For instance, while investigating the source of Stuxnet, a malware that was designed to sabotage Iran's nuclear enrichment facility³², analysts took into account various facts including an article published by a former US intelligence officer one year prior to Stuxnet being discovered, outlining a strategic cyber strike against centrifuges, and the high level of sophistication in the software to conclude that the US government was involved.³³ Another example is the United States indictment of the 5 PLA members in *United States v. Wang Dong et al.*, which was partly based on identifying signatures or hallmarks in the

³⁰ Roscini, supra note 6, at 251.

³¹ Ibid.

³² Kim Zetter, 'An Unprecedented Look at Stuxnet, the World's First Digital Weapon', WIRE, March 11, 2014, [1–2] <<https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/>>.

³³ Paul Mueller and Babak Yadegari, 'The Stuxnet Worm' (University of Arizona) <<https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/2012/topic9-final/report.pdf>>.

malware, in addition to the time pattern of their activities corresponding with the business hours in Shanghai.³⁴

4 The Corfu Channel rule: when circumstantial evidence was “Good Enough”

As far as international law is concerned, circumstantial evidence is commonly used and has sometimes even been sufficient to find states responsible for violations. In the very first dispute before it, the *Corfu Channel* case, the ICJ had to deal with issues involving circumstantial evidence provided by the United Kingdom (“UK”) and exclusive control of evidence by Albania. In the case, the UK alleged that Albania had knowledge of and failed in its obligation to warn the UK of the mines in its channel which struck two UK warships. With regard to the indirect or circumstantial evidence provided by the UK, the Court ruled that “proof may be drawn from inferences of fact provided they leave no room for reasonable doubt”.³⁵ After acknowledging that the UK did not have access to evidence that was within Albania’s exclusive territorial control and was hence disadvantaged by it, the Court allowed it a “more liberal recourse to inferences of fact and circumstantial evidence.”³⁶ By establishing that Albania closely guarded the channel waters, could observe the mine-laying from the Albanian coast, and providing evidence of previous Albanian mine-sweep operations, the UK was able to establish “a series of facts linked together and leading logically to a single conclusion”³⁷ that in the Court’s opinion left “no room for reasonable doubt” that Albania knew about the mines in the channel,³⁸ and hence, violated its obligation to warn the UK. Other facts that corroborated the UK’s claim included a declaration by the Albanian delegate in the Security Council and diplomatic notes from Albania on the passage of ships through its territorial waters.³⁹

The *Corfu Channel* case shows that the Court allows “recourse to liberal inferences of fact and circumstance” to prove state responsibility when (a) the relevant direct evidence is within the exclusive territorial

³⁴ *United States of America v. Wang Dong, et al.* (Crim. No. 14-118 W.D.Pa.)

³⁵ *Corfu Channel Case, Judgement of April 9th, 1949* : I.C.J Reports 1949 at 4 [18].

³⁶ *Ibid.*

³⁷ *Ibid*

³⁸ *Ibid* at 22.

³⁹ *Ibid* at 19.

control of another state and (b) the circumstantial evidence furnished is consistent with or does not contradict any direct evidence produced.⁴⁰ But cyber attribution experts would do well to note that it was simply the method of proof that was relaxed in this case, and not the standard of proof. Even in cases where such circumstantial evidence is allowed to be adduced, it would still have to sufficiently meet the requisite standard of proof or threshold, which in the *Corfu Channel* case was characterized as “no room for reasonable doubt”. Hence, applying this to the cyber-domain can mean that the lack of evidence could allow for a lower method of proof, but the standard of proof remains high.

While the *Corfu Channel* rule is regularly cited as the prevailing standard on the treatment of circumstantial evidence in international law, the ICJ’s *Bosnian Genocide* case is often cited as the decision in which the Court rejected the argument that circumstantial evidence was sufficient to fix state responsibility. But the Court’s ruling in this case was for different reasons.

5 The Bosnian Genocide case: when circumstantial evidence was not “Good Enough”

In the *Bosnian Genocide* case, Bosnia and Herzegovina alleged that Serbia had violated the prohibition on genocide under the Genocide Convention and had also failed in its obligation to prevent and punish the perpetrators of genocide.⁴¹ Similar to the UK in *Corfu Channel*, Bosnia also argued that Serbia had exclusive territorial control over the territory making it almost impossible for it to produce direct evidence showing Serbian complicity and that the Court should allow Bosnia to make liberal inferences of fact and circumstance from patterns of evidence to hold Serbia responsible for and also having the specific intent of carrying out the genocide⁴², i.e., the Court should use circumstantial evidence to come to a positive finding of specific intent on Serbia’s part. But the Court refused to do so and held that for the

⁴⁰ Michael P Scharf and Margaux Day, ‘The International Court of Justice’s Treatment of Circumstantial Evidence and Adverse Inferences’ (2012) 13 Chicago Journal of International Law 123.

⁴¹ *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*, Judgment, I.C.J. Reports 2007 at 43 [65].

⁴² *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*, Memorial of Bosnia & Herzegovina, 216-17, 5.3.3.8 (April 15, 1994).

requisite intent to be proven, any pattern of conduct would have to “be such that it could *only point* to the existence of such intent.”⁴³

With regard to the Court rejecting circumstantial evidence in this instance, a number of factors played a role. One factor was that Serbia presented a lot of direct evidence to the contrary, such as witness statements. The ICJ also relied on the ICTY’s judgements which contained findings of fact that went against what Bosnia was trying to prove.⁴⁴ Given this, it is hard to take the view that the Court has moved away from the *Corfu* rule on circumstantial evidence. Clearly the Court *prefers* direct evidence, as would any judicial forum, but this is not to say that in cases where such direct evidence may be *absent* either due to technical difficulties or the refusal of a party to produce it, the Court will not turn to circumstantial evidence.

6 Other international legal Jurisprudence

Circumstantial evidence has also found common use in other international forums. For instance, the Eritrea-Ethiopia Claims Commission in its *Partial Award for the Central Front, Involving Eritrea’s Claims 2, 4, 6, 7, 8, and 22*,⁴⁵ held Ethiopia liable on the basis of the testimony of a civilian who testified that a cemetery that had been undamaged before he fled the village before Ethiopian troops arrived, was found destroyed after he returned. The inference from this testimony, together with the fact that the village was under Ethiopian control, was used by the Commission to conclude that Ethiopia responsible.⁴⁶

Similarly, the NAFTA tribunal in *Methanex v. United States* was “not averse to trying to connect the dots”⁴⁷ put forth by Methanex to examine whether they led to the “most compelling of possible explanations of events”⁴⁸ and conclude that the United States was in violation of its obligations under the NAFTA. While the Tribunal ultimately concluded

⁴³ *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*, Judgment, I.C.J. Reports 2007 at 43 [196-97, 373].

⁴⁴ *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*, Judgment, I.C.J. Reports 2007, at 43 [131].

⁴⁵ Eritrea-Ethiopia Claims Commission, *Partial Award, Central Front, Eritrea’s Claims 2, 4, 6, 7, 8 & 22*, (Apr 28, 2004).

⁴⁶ Eritrea-Ethiopia Claims Commission, *Partial Award, Central Front, Eritrea’s Claims 2, 4, 6, 7, 8 & 22*, (Apr 28, 2004) at 16–17, 71.

⁴⁷ Eritrea-Ethiopia Claims Commission, *Final Award of the Tribunal*, 44 ILM 1345 (Aug 3, 2005), Para 57, Part 3, Chapter B-Page 26.

⁴⁸ *Ibid* at Part III- Chapter B- Page 1, 2.

that the “dots” together did not point to liability on the part of the United States⁴⁹, it is a good example of the use of inferences or circumstantial evidence in international law, particularly since the NAFTA tribunal relied on the same sources of law as the ICJ, specified in Article 38(1) of the ICJ Statute.⁵⁰

7 Cyberspace attribution: current status in brief

Most digital forensic data available to analysis experts in the aftermath of cyber-attacks are in the form of IP addresses, email addresses, domain names, hashes, etc. which are analysed to answer the *what*, *how*, *who* and *why* questions. Much of this currently involves educated guesswork which includes examining samples such as malware or custom tools found in the affected cyber-infrastructure, or identifying language and content patterns found in phishing emails, determining locations of servers and so on to answer the *what* and *how* questions. This then needs to be viewed in combination with other evidence typically obtained from signals intelligence, human intelligence, etc. to form a clearer picture of the *who* and *why* questions.

For instance, the US indictment of 5 PLA members in *United States v. Wang Dong, et al.* was based, apart from digital forensic data including patterns in spear-phishing emails, on facts such as the target / victim companies all having significant economic or business interests in China as well as the period of activity by the accused corresponding to business hours in Shanghai.⁵¹ While this is an example of the use of the “connect the dots” method in cyber violations, it happens to be a far cry from the “fully conclusive”, “clear and convincing” or the “no room for reasonable doubt” standards of evidence required in state-to-state litigation. Indeed, the indictment is only the first step in domestic criminal proceedings and even within the United States, the accused in this case are innocent until they are proven guilty in a court of law.

In the cyber sphere itself, there have so far been multiple private investigative attempts to attribute cyber-attacks or identify malicious cyber actors. Some examples are the Project Grey Goose Report on the Georgia DDOS attacks which indicates that the attacks originated from Russia and that they were also possibly supported by the Russian

⁴⁹ Ibid at Para 60.

⁵⁰ Ibid at Part II- Chapter B- Page 1.

⁵¹ *United States of America v. Wang Dong, et al.* (Crim. No. 14-118 W.D.Pa.).

government⁵², and the Mandiant Report which traces and identifies a cyber unit in the PLA as the main perpetrator in multiple cyber-attacks and cyber-espionage in the United States.⁵³ Despite the technical detail in these Reports, the connections drawn by them from inferences or “dots”, so to speak, to link the perpetrators to the states, are tenuous and not likely to meet legal thresholds. At best, these reports may be viewed as corroborative evidence and are otherwise not likely to withstand scrutiny in any international judicial forum.

8 Circumstantial evidence in context

Having noted that gathering circumstantial evidence is difficult, let us contextualize the use of circumstantial evidence to prove state responsibility in the cyber-domain. Taking the malicious cyber-activity in one of India’s nuclear reactors at Kudankulam as an example, investigations have reportedly revealed that (i) the attack was traced to a computer model that is produced in and only used in North Korea, (ii) that the MAC and IP addresses bear North Korean signatures, (iii) that the Korean language was used in the code, (iv) the malignant code corresponded with a previous cyber-attack on South Korea’s banks that was also attributed to North Korea and lastly (v) that the code is a variant of the “Dtrack” malware known to be associated with the Lazarus Group believed to be composed of North Koreans.⁵⁴ Add to the mix other “circumstances” such as the highly state-controlled nature of North Korean cyberspace and reports of a cyber-warriors trained by the North Korean government used to carry out similar cyber espionage operations in different countries. Based on this information, it is certainly tempting to point the finger at the North Korean government for the Kudankulam cyber-attack and many have.⁵⁵

But still, by itself this evidence is not likely to achieve much at the ICJ. It is doubtful that these facts, even if proved, would be construed as

⁵² Project Grey Goose, *Russia/Georgia Cyber War—Findings And Analysis (Phase I Report)* (2008), <<https://www.scribd.com/doc/6967393/Project-Grey-Goose-Phase-I-Report>> accessed 11 February 2020.

⁵³ Mandiant, *Threat Report* (2014), <https://dl.mandiant.com/EE/library/WP_M-Trends2014_140409.pdf> accessed 11 February 2020.

⁵⁴ Saikat Datta and Andrew Salmon, ‘North Koreans behind Indian Nuclear Plant Hack’, *Asia Times*, November 12, 2019, [14–25] <<https://www.asiatimes.com/2019/11/article/north-koreans-behind-indian-nuclear-plant-hack/>>.

⁵⁵ Prabhjote Gill, ‘Here’s Why North Korean Hackers Attacked India’s Nuclear Power Plant’, *Business Insider India*, November 13, 2019, [1] <<https://businessinsider.in/tech/news/heres-why-north-korean-hackers-attacked-indias-nuclear-power-plant/articleshow/72035492.cms>>.

constituting “a series of facts linked together and leading logically to a single conclusion” leaving “no room for reasonable doubt” as in the *Corfu Channel* case. India would not just have to prove that the malware was traced to North Korea, she would also be required to negate the possibilities of IP spoofing, code-mimicking and other modes of concealment and disguise in cyberspace since it will bear the burden of proving its claim. In fact, if it were to rely on this kind of circumstantial evidence, India might also be required to prove facts such as the malware being of a kind that *only* the North Korean government possesses and uses with no reasonable possibility of any other actor having access to it, and that the North Korean government stands the most to gain to the exclusion of any other state or actor. Obviously this is a very high burden on any state. Considering most of the evidence is likely to be in the exclusive control of North Korea, would India be allowed liberal recourse to facts and circumstance? Possibly. But such recourse would still be circumscribed by the requirement of meeting the high “no room for reasonable doubt” standard. And it is that high standard that India is not likely to meet, unless more evidence sees the light of the day.

9 Conclusion

Despite the law almost never functioning within the boundaries of absolute certainty, it is apparent that the “good enough” standard currently touted as sufficient for public attribution or for taking countermeasures⁵⁶ is definitely not going to cut it for states that wish to seek reparations or other legal reliefs in any international court, particularly the ICJ. Even the Tallinn Manual 2.0 recognizes this when it cautions that if the conclusion as to attribution proves to be flawed, the State responding to the cyber-attack with countermeasures will itself have committed an internationally wrongful act.⁵⁷ As for ongoing efforts to lower the threshold for attribution in case of non-state actors from the prevailing test of “effective control” to the test of “overall control” or even form entirely new tests such as the “control and capabilities” test, it should be noted that no matter what the attributive test, the evidentiary standard of proof remains high and the methods of proof in cyberspace difficult to navigate.

⁵⁶ Shane McGee, Randy V Sabett and Anand Shah, ‘Adequate Attribution: A Framework for Developing a National Policy for Private Sector Use of Active Defense’ (2013) 8 *Journal of Business & Technology Law* 48, 25.

⁵⁷ Schmitt, *supra* note 28, at 83.

Rapid modernization, along with the ongoing Covid-19 pandemic, has both spurred and highlighted the importance of the digital world as well as its supporting infrastructure. It is no surprise that cyber operations are currently high on the agenda for most States. Estonia's recent presidency of the United Nations Security Council saw cyber-attacks being raised for the first time as an issue at the Security Council.⁵⁸ In a bid to stay ahead, States are racing against technological progress by attempting to identify norms for responsible state behaviour in cyberspace. This effort has already led to broad agreement (barring a few States) that conventional *jus in bello* or the law of war is applicable to cyberspace and cyber-attacks.⁵⁹ There is also broad consensus that concepts of *jus ad bellum* such as the prohibition of the threat or use of force and the right to self-defence under Article 2(4) and Article 51 of the United Nations Charter, 1945, respectively, are also applicable to cyberspace.⁶⁰ Even though States are still in the process of agreeing on the modalities of how these rules apply, surely there can be little question that the evidentiary rules of *proving* the violation of these obligations must simultaneously receive serious consideration. After all, standards of proof and methods of proof are not decided by States, but the judicial forum deciding contesting claims. As States engage in the all-important task of fleshing out the rules for applying conventional legal obligations in cyberspace, it is important for them to bear these issues in mind. Technical experts and strategists involved at all levels of attribution must necessarily be mindful of evidentiary hurdles so they may be guided in determining how much information / evidence is required to make attribution meaningful.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

⁵⁸ 'The Estonian Presidency of the UN Security Council Holds a Landmark Discussion on Cybersecurity' (Permanent Mission of Estonia to the UN, 21 May 2020) <<https://un.mfa.ee/the-estonian-presidency-of-the-un-security-council-holds-a-landmark-discussion-on-cybersecurity/>> accessed 8 July 2020.

⁵⁹ 'Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (n 17).

⁶⁰ Ibid.