Error 404: Responsibility Not Found? Evidentiary Dilemmas in Attributing Cyber Operations

opiniojuris.org/2022/08/24/error-404-responsibility-not-found-evidentiary-dilemmas-in-attributing-cyber-operations

August 24, 2022

[Abhijeet Shrivastava is a fifth-year law student at Jindal Global Law School, India.]

Introduction

The emergence of cyberspace has invited countless international legal complications. Debates loom over novel questions concerning the interaction of the new technological terrain with existing thresholds for breaches of international legal commitments. Yet in addition, to prove a State's "responsibility" for allegedly wrongful acts, a *sine qua non* is showing that the conduct in question was "attributable" to that State [Articles on the Responsibility of States for Internationally Wrongful Acts, art. 2 ("ARSIWA")].

Cyberspace poses evidentiary difficulties in establishing attribution, given the growing frequency of covert cyber operations, as well as the technological capabilities or even inter-State cooperation required to secure necessary evidence. This may be relatively easier in case the acts were performed by the *de jure* or *de facto* organs of a State (see ARSIWA arts. 4-7) or if the State itself acknowledges and adopts the conduct as its own (ARSIWA art. 11). However, victim States may be in especially precarious positions when

faced with cyber operations conducted by private actors. To show attribution for otherwise private acts, victim States would have to meet the onerous factual test of another State's "instruction, direction or control" in respect of such acts (ARSIWA art. 8).

In this piece, focusing on International Court of Justice ("ICJ") case-law, I will unpack the implications of the Article 8 test for cyber operations. I will also draw from the limited *opinio juris* currently available from States that have elaborated their positions on how international law applies in cyberspace. Simultaneously, I consider whether there may or even should arise a less onerous *lex specialis* test for attributing cyber operations.

The Test For Attribution

The ICJ considered Article 8 of the ARSIWA to reflect customary law in the *Bosnian Genocide* case of 2007 (¶398). To begin with, it is important to acknowledge that there are two *distinct* tests provided in Article 8. Showing that private acts were carried upon the "instructions" of a State can *in se* prove attribution. For example, if a State hires a private corporation to conduct defensive cyber operations on its behalf, the entity would be akin to 'auxiliaries' – and thus, its corresponding conduct would be attributable to the State [see for scholarly discussion, the Tallinn Manual 2.0 on the law applicable to cyberspace, p. 95 ("Tallinn Manual")]. However, the test of "instructions" is evidently tailored to a very limited context and not frequently invoked. This is different from the test of "direction or control" mentioned in the same Article. While some consider "direction" and "control" to *also* be disjunctive tests (ARSIWA commentaries, p. 48), these terms have been used conjunctively and interchangeably by most international fora (p. 146).

According to the ICJ's *Nicaragua* Merits judgment of 1986, such State control must be "effective" – in that the State must have *"enforced and directed" each* act alleged by a claimant State (¶115). A factual inquiry is required to establish this extent of control in each case. The United States' ("US") giving of military intelligence, extensive financial and logistical support for rebels acting against Nicaragua *failed* to meet this stringent test, even when appropriate targets for raids were shared (¶¶105-106). The test of effective control has never been met before the ICJ and rarely, if ever, before other fora (p. 80-81). In the *Bosnian Genocide* case, the ICJ was asked to uphold the more relaxed test of "overall control" proposed in the *Tadić Appeals* judgment (1999) of the International Criminal Tribunal for the Former Yugoslavia. Under that test, conduct such as the US' in *Nicaragua* could have given rise to attribution.

Yet the Court upheld the "effective control" test as reflecting customary law, arguing that more lenient tests would blur the lines between private and State action (¶¶402-404). As per the Tallinn Manual, this remains the test applicable to cyber operations (Rule 17).

The ICJ's Evidentiary Approaches

Before proceeding further, it is helpful to recall some general evidentiary points emerging from the ICJ's jurisprudence. In doing so, let us look at three different issues: that of the "burden" of proof, the "method" of proof, and the "standard" of proof (see here for an extensive discussion). The first term concerns which party bears the charge of *proving*

certain facts – the ICJ has held that as a general rule, the party "asserting" a fact must prove its existence [see *Pulp Mills* at ¶162 (2010); *Nicaragua* Jurisdiction judgment at ¶101 (1986)]. Thus, victim States bear the burden to prove a link of attribution as aforementioned. Second, the "method" of proof considers the *nature* of the evidence to be presented – i.e., direct, or indirect (circumstantial). In *Corfu Channel* Merits (1949), the ICJ encouraged "liberal recourse" to the circumstantial evidence presented by the United Kingdom in proving Albania's knowledge of the presence of mines in its waters (p. 18). This was since Albania exercised "exclusive" control over its waters, precluding the United Kingdom from securing any "direct" evidence (p. 18). Accordingly, as Aravindakshan argues, States victim of cyber operations will likely be allowed to base much of their case on circumstantial evidence, since that *is* the method of proof most accessible to them.

However, this is where the third term – the "standard" of proof gains prominence – in that the ICJ only affirmed the United Kingdom's claim because the evidence left "no room for *reasonable doubt*" (p. 18). This concerns the measure by which the evidence must persuade the Court as to the existence of certain facts. This is why, even when Bosnia and Herzegovina was in a similar situation, the Court declined some of its allegations because the circumstantial evidence was contradicted by competing direct evidence (Bosnian Genocide, ¶131; Aravindakshan, p. 295). Further, in the same case, which involved allegations of genocide, the Court held that it would employ a higher standard of proof for charges of "exceptional gravity" – in that case, of "fully conclusive" evidence (¶209).

Indeed, as per Dr Rajput, the Court has not followed a consistent standard of proof, varying its scrutiny based on the claims at hand to different standards – such as the preponderance of probabilities, fully conclusive evidence, convincing evidence, and so forth. To elaborate in respect of *Nicaragua*, the Court appeared disinclined to rely on circumstantial evidence for imputing the rebels' actions violating humanitarian law to the US, including civilian killings (¶¶113-115). Therefore, the seriousness of the legal allegations made by the State may also play a part in the attribution of the cyber operations to another State; and even in proving the very existence of the cyber operations to begin with. All this does seemingly put claimant States in a difficult position. Yet is that necessarily a problem, and what have States said about cyber attribution?

A *Lex Specialis* Test For Cyberspace?

I take this occasion to respond to Peter Stockburger's suggestion in a 2017 article that a new special test may be crystallizing in customary law for attributing cyber operations – what he called the "control and capabilities" test, which would be even more relaxed than the "overall control" test (Aravindakshan, p. 287). To be clear, this test would not affect the burden, method, or standard of proof as explained above – but rather the *very facts* that need to be proven to show a factual link of attribution. There would not be a need to show "effective" control, but rather, a few sets of circumstances, such as the private group and the State's locations, common motivations, technical capacities, the State's influence over the group, and so forth (p. 1). In making this claim, he primarily cites three instances of public attribution of cyber operations between 2014-2017, *all* by the US against North

Korea, Russia and Iran respectively. In apparently relying on the 'specially affected States' logic for contending the development of customs, he argues that support for new norms need not be universal, and great weight can be given to the practices of affected States that have "influence in a particular area" (p. 8).

There are many problems with this argument. To begin with, let us consider the 2021 statement of the US as recorded in a Compendium released by the United Nations Group of Governmental Experts concerning cyber-law ("Compendium"). This statement draws from a 2016 speech of US Legal Adviser Brian Egan. There, the US has instead affirmed the general "direction or control" test (rather than any *lex specialis*); and has argued that the ARSIWA nowhere sets "burdens or standards of proof for attribution…Such questions may be relevant for judicial or other types of proceedings, but they do not apply…to a State's [unilateral] determination about attribution…for purposes of its response" including countermeasures (p. 141). There is no need to unpack here the merit of its suggestion that there is no strict evidentiary burden to support self-help when a victim State "acts as its own Judge" (p. 141). It suffices to note that the practices Stockburger cites should not be given their alleged weight, given the US' clarification that its statements are without prejudice to judicial evidentiary standards.

More importantly, the doctrine of 'specially affected States' has faced great criticism for being a suspicious device through which the most powerful States from the Global North could translate their common self-interests as the applicable law – here, primary reliance on US practice gives rise to similar apprehensions. Even if accepting this concept, and if the principle of equality of States is to remain relevant, it is more appropriate to consider practices of States that have a special *legal* interest in a field rather than those having the most "influence" as Stockburger suggested (p. 8). In that regard, one must be cautious in relying on existing *opinio juris* on cyberspace as it only comprises a few dozen States. The cyberspace is, after all, of important concern and interest to almost all States, given its contemporary reach, even if only a few States have clarified their legal views around it.

In any case, returning to the suggestion of a *lex specialis*, most outspoken States (i.e., taking a position on the issue) have now affirmed that it is the traditional test of "effective control" or instructions as per Article 8 that applies to private cyber operations. From the UNGGE Compendium, this includes the views of Australia, Brazil, Estonia, Germany, Japan, the Netherlands, Norway, Romania, Russia, Singapore, Switzerland and the United Kingdom – with other States such as Finland affirming this on separate occasions. Furthermore, Brazil (Compendium, p. 21) and Finland (p. 5) have specifically rejected the contention that a *lex specialis* has arisen regarding attributing cyber operations. One must remember that cyber operations are becoming increasingly financially expedient, such that corresponding responsibility of private groups is also becoming more likely as a suspected possibility. Thus, as Roscini suggests, the likelihood of "false attribution" is high in cyberspace, perhaps necessitating sticking to the conservative tests of attribution. That is, at least until there is more to learn from a hopefully representative set of future *opinio juris*.

Concluding Remarks: Indirect Responsibility

What then, are victim States to do until clearer *opinio juris* emerges? There is already extensive scholarly literature, including the majority consensus in the Tallinn Manual itself, on principles such as the non-intervention prohibition and that of due diligence, which can attract State responsibility even *absent* attribution of private conduct. That was also the case in *Nicaragua*, where the US' support to the contras violated the non-intervention principle (¶292.3; since the *support* itself was attributable). Due diligence would also operate, *inter alia*, for the States' failure to prevent harm against other States when caused by private groups in their jurisdiction. Apart from legal proceedings, the invocation of even such internationally wrongful acts could also justify taking self-help measures such as countermeasures on a case-to-case basis. Of course, there could be valid dissatisfaction with this route in that it could enable deniability of attribution. Yet, we must wait for representative State consensus on cyber-law in this context. The increasing openness of States on this count is encouraging, to which scholarly contributions remain pertinent.