Bangladesh Society of International Law

A PUBLICATION OF BSIL

Bangladesh Blog of International Law

Connecting Bangladesh to International Law

ARTICLE

When Attribution Becomes a Legal Escape Hatch_The Problem with Attribution

17 August 2026 | By **Abrar-Bin-Shoukat Alvi**

The Problem with Attribution

According to standard state responsibility rules, a state is liable only when any conduct is attributed to it and breaches any international obligation. However, cyber operations are very hard to trace. Because attackers use botnets, proxies, and hacked systems across multiple countries. (France Diplomatie, first published 2019, updated 23 July 2026). All states do not have the same or similar ability to solve this difficulty. Countries with advanced forensics, intelligence, and investigative capacity can easily turn technical evidence into legal proof. On the contrary, states with lower resources struggle to do this. (Tsagourias and Farrell, 2020).

The Bangladesh Bank cyber heist of 2016 is a significant example of this asymmetry. US prosecutors alleged that a North Korean-sponsored hacking group was responsible for the theft of $81 million from Bangladesh Bank (US Department of Justice, 2018). The US Department of Justice account is based on their own multi-year investigation, which is not an international legal decision. This example illustrates that investigative capacity determines when an attribution becomes practically usable. Therefore, this article proposes two tracks which are the direct attribution as the primary route, and the due diligence as a secondary route based on the State's own failure to comply with an applicable due-diligence obligation.

The rules for the first track are governed by ARSIWA. As per article 2, it is required to prove the link to the state, as well as the breach of international law. Articles 4 and 7 cover state organs, even if they act beyond their authority. Again, article 8 applies when private persons act under the instructions, direction, or control of a state. If a state later acknowledges and adopts the conduct as its own, the conduct becomes attributable to that state under Article 11.

© 2026 Bangladesh Society of International Law (BSIL). All rights reserved.

Therefore, when a state functions through non-state proxies, it becomes harder to connect them legally. Technical evidence, political accusation, and legal attribution are not the same things. Strong technical proof alone is not enough to prove state responsibility. Consequently, victim states have to choose either a weak remedy or a forceful response without enough legal backups.

Why Non-Intervention Matters More Than Force

The use of force is prohibited by Article 2(4) of UN Charter, which makes it a natural starting point. But the threshold where a cyber operation becomes force remains disputed. Operations that cause physical injury or damage are the clearest cases of force. However, non-destructive disruptive cyber attacks remain disputed. (Roscini, 2015) So, quite a few harmful cyber attacks fall below that force threshold.

In such cases, the prohibition on intervention may be more useful. The Friendly Relations Declaration rejects both direct and indirect intervention. In the Nicaragua case, the ICJ held that coercion is the main element of prohibited intervention (Nicaragua, para. 205; Friendly Relations Declaration, UNGA Res 2625 (XXV)). Cyber operations are also able to affect the sovereign choices of a state.

Manipulating elections, disrupting financial systems, or targeting medical services can be prohibited intervention following the UK Cyber statement. Only serious harm is unable to prove illegal intervention. It is necessary to show that coercion was directed at a matter within the sovereign choice of the target state. (Pomson, 2022).

BANGLADESH SOCIETY OF INTERNATIONAL LAW

A Second Track Through Due Diligence

Attribution should be the primary route for state responsibility. Standard ARSIWA rule applies when state organs act or private actors operate under state control. Technical advancement is unable to change this legal framework. The initial deployment remains attributable to the original state, if malware is later modified or spread by others. The separate question is whether later effects are sufficiently connected to that state for legal breach and responsibility or not.

The second track addresses own failure or omission of the state. This becomes significant when the victim state is unable to prove direct state control over the attacker. However, the victim state needs to show that the other state failed to take reasonable measures in order to prevent the act. In the Corfu Channel, the ICJ recognised the obligation of a State not knowingly to allow its territory to be used for acts contrary to the rights of other States.

The main objection is that a specific cyber obligation lacks universal consensus. For instance, the UK considers it non-binding but the Netherlands recognizes it as a due diligence duty in cyberspace (UK cyber statement, 2021, para. 12; Netherlands position, 2019, pp. 4–5). The solution is not to declare a universal duty when cyber harm occurs. Rather, scholars Coco and de Souza Dias highlight existing obligations across human rights and international laws. Accordingly, the second track need not depend on a freestanding universal cyber due-diligence obligation. It can operate where an existing international obligation binding on the State entails a due-diligence standard.

Knowledge and capacity are central here. The question is whether the state knew or should have known of a risk and failed to take reasonable measures. The necessary conduct depends on capacity because a state cannot be forced to do anything impossible for it (Coco and de Souza Dias, 2021, pp. 788–789). Therefore, harm alone is not enough to establish liability. The claimant has to prove the legal obligation along with the territorial link, knowledge, and inaction.

It is necessary to check whether the state investigated a notice, saved data, or warned affected parties. It is also important to check whether they cooperated lawfully, disrupted infrastructure, or reduced ongoing harm. However, the Tallinn Manual 2.0 or NIST Cybersecurity Framework 2.0 are not binding international law.

Again, public disclosure must be separated from responsiveness (UK cyber statement, 2021, para. 15). A state which is making an attribution is under no legal obligation to publish its underlying evidence. Failure to respond may be relevant evidence, but it alone is not enough to prove guilt, breach, or responsibility.

This distinction is very important when applied to Bangladesh Bank. This incident shows the first-track difficulty of making and using attribution. However, this incident alone does not prove a due diligence breach by any state without extra proof. To make a second-track claim, one must identify the specific obligation binding to the state. Also, one must prove whether the state knew about it and specify the possible preventive or cooperative measures required. And, it must be shown that the state failed to take those steps.

Why This Debate Is No Longer Academic

Policy on cyber-enabled crimes issued by the ICC Office of the Prosecutor explains that cyber-enabled action may fall within the existing Rome Statute crimes when jurisdictional elements are met. Consequently, common cybercrime does not automatically convert to an international crime, and individual international criminal responsibility remains separate from state responsibility. Nevertheless, the policy ensures that established legal

regimes must be able to handle complex tech conduct without dropping their main rules.

The goal is neither to weaken attribution, nor invent liability whenever serious cyber harm occurs. Rather, attribution should remain primary where state conduct can be legally established. However, failure of attribution should not automatically result in closure of the inquiry. When a state is in a position that it knew or should have known of the risk and failed to take reasonable measures, responsibility may arise for its own omission. Again, the second track simply prevents attribution from becoming a legal escape hatch.

BANGLADESH SOCIETY
OF INTERNATIONAL LAW