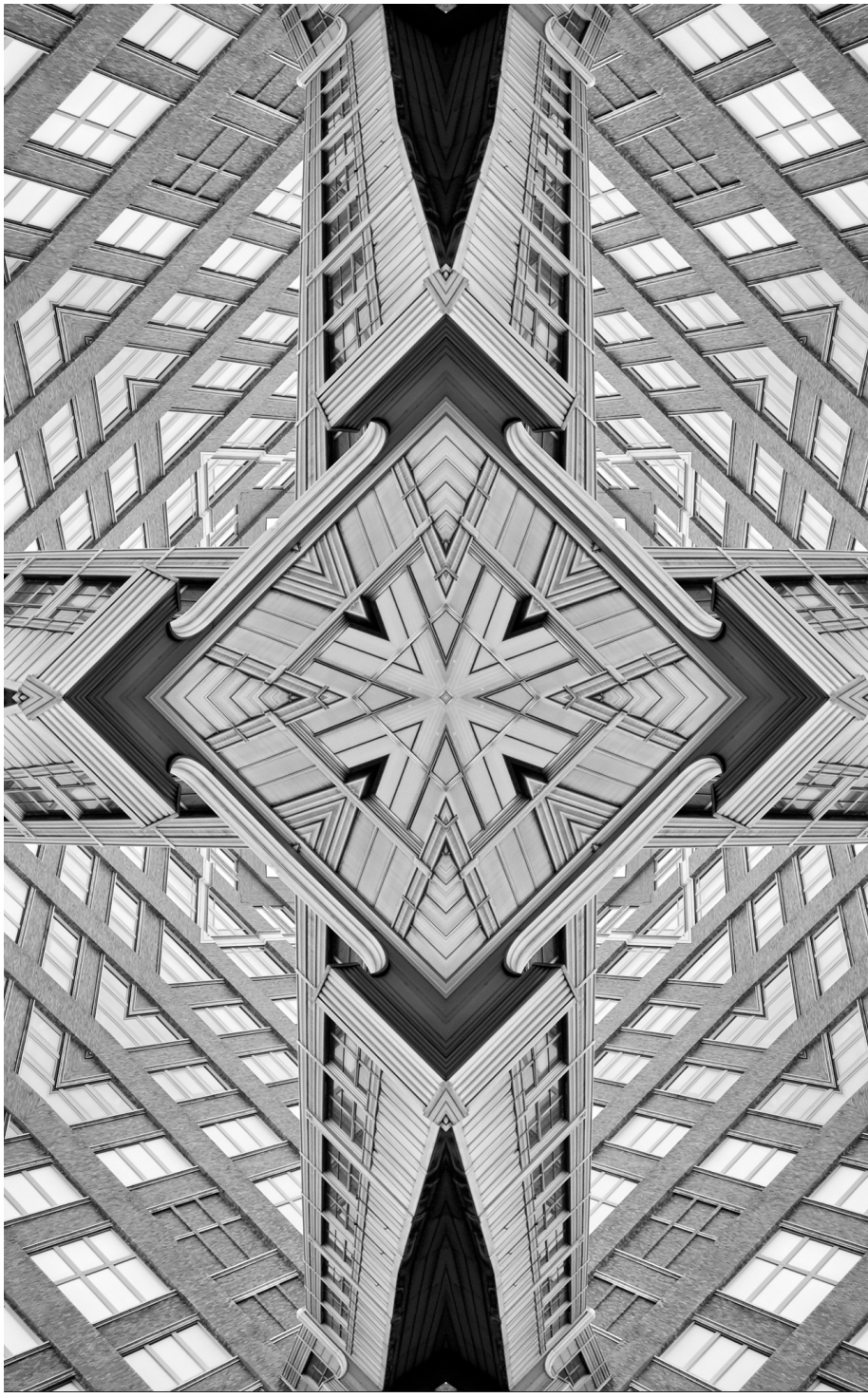
# Issue Brief

ISSUE NO. 748
NOVEMBER 2024

ORF OBSERVER RESEARCH FOUNDATION



# International Cyber Incidents: On the Question of Public Attribution

**Arindrajit Basu**

The public attribution of a cyber incident—undertaken coherently and underscored by robust decision-making—can be a useful tool for national security. India, thus far, has not publicly attributed any international cyber incident to a specific private perpetrator or nation-state. Studying the models framed by scholars based in other jurisdictions, this brief offers suggestions on how India can approach the issue of public attribution of cyberattacks. Based on existing criteria, if a decision to publicly attribute is made, the brief proposes the following options, either individually or in combination, for Indian decision-makers: criminal indictment; international legal attribution; political attribution; and relying on third-party attribution.

Attribution: Arindrajit Basu, "International Cyber Incidents: On the Question of Public Attribution," *ORF Issue Brief No. 748*, November 2024, Observer Research Foundation.

# Introduction

We live in an age of cyber 'unpeace'[1] where modern mid-spectrum rivalry "fits neither the destructive criteria [and violence] of war nor the acceptable boundaries of peace."[2] The blurring of cyber boundaries brought about by asymmetry allows both states and nation-states to attain international economic and geopolitical objectives without engaging in traditional kinetic warfare.

This new reality compels holistic and cohesive thinking from policymakers across the world on how to exploit opportunities and minimise threats posed by the pervading uncertainty of cyber 'unpeace'. International cyber operations, frequently undertaken by states, state-backed actors, or independent non-state actors, provide asymmetric advantages to entities that may not boast traditional military or technological power. The many challenges of effectively attributing attacks to a perpetrator or group compounds geopolitical uncertainty.

Existing literature documents the technical constraints on attribution. Cyberattacks span stages, steps, and jurisdictions.[3] This adds several layers of complexity to the attribution process. The system deploying the offensive capability is usually several degrees removed from the computer or computer network being infiltrated. Attackers can obfuscate their activities using different technical means like botnets, spoofing, and false flag techniques to deceive the forensic analyst; they can also use proxy networks.[4] While states or private actors can likewise use varied technical means to trace the attack's origins, accurate attribution remains a cumbersome and challenging process.[5]

Indeed, some experts argue that attribution is as much an art as it is a science.[6] No technical cyber forensic analysis can fully solve the attribution challenge in cyberspace. Other analysts have, however, highlight the benefits of public attribution. Researchers at the RAND Corporation are of the view that public attribution furthers credibility, enables information exchange that improves the quality of attribution, and can potentially deter future adversaries by signalling that existing mechanisms can detect and retaliate against attacks. Still others are more circumspect about these benefits[7] and highlight the potential costs of public attribution, including misattribution and escalation.[8]

# Introduction

Scholarship published in the past two years recognises both arguments and suggests frameworks to guide decision-makers on publicly attributing cyber incidents.[9] As noted by the editors of an ORF monograph on emerging technologies and future warfare,[10] the transformation of warfare in the age of unpeace demands an arsenal of strategic options to counter cyber incidents and secure India's burgeoning digital economy. Public attribution, guided by sound decision-making, can be useful. Thus far, India has not publicly attributed a specific international cyber incident to a specific private perpetrator or nation-state. This brief applies the models created by Western scholars to outline suggestions on how India can view the question of public attribution of cyberattacks.

# The Cyber Threat Landscape in India

Increased digitisation, combined with the country's geopolitical location amid two adversarial neighbours, makes India vulnerable to cyberattacks.[11] According to a report from Check Point Research, organisations in the country faced an average of 2,108 cyberattacks weekly in the first quarter of 2023, marking a 15-percent increase from the same period in previous years.[12] Critical infrastructure has often been at the receiving end of cyberattacks. Notable ones[13] include the Cosmos bank fraud in 2018 where a malware attack authorised fraudulent transactions, causing the bank to lose INR 94 crore;[14] the D-Track malware attack in 2019 that breached the Kudankulam reactor's administrative network;[15] and in 2022, the disruption of the IT network of AIIMS, one of India's leading government-run hospitals.[16]

Officials have acknowledged that finding the necessary evidence to attribute cyberattacks to a specific perpetrator is a massive challenge.[17] Lt. General Rajesh Pant, India's former National Cybersecurity Coordinator, has particularly highlighted the hurdles posed by the Mutual Legal Assistance Treaty (MLAT) process in obtaining information from international partners.

India came close to a public attribution in 2018 when a report shared with the National Security Council Secretariat by CERT-In claimed that 35 percent of cyberattacks on official Indian websites originated from China, followed by 17 percent from the United States (US), 15 percent from Russia, 8 percent from Pakistan, 7 percent from Canada, and 5 percent from Germany.[18] However, the full report, along with any accompanying evidence, is not in the public domain and information can only be gleaned from media reports. It is therefore unclear whether CERT-In has attributed specific attacks to specific perpetrators or countries.

Indeed, politicians and authorities have made a conscious effort not to name the perpetrator or state of origin when acknowledging and characterising cyberattacks or attempts to conduct cyberattacks. For example, the government explicitly denied a Chinese role in a cyberattack in 2020 that temporarily brought down the Maharashtra electricity grid, despite findings by threat intelligence company Recorded Future suggesting that it was the case.[19] With the more recent AIIMS cyberattack, in a written reply to the Rajya Sabha, Minister of State Rajeev Chandrashekhar forensically characterised the "sophisticated ransomware" attack and claimed it was a "conspiracy and planned by [significant] forces."[20] He also divulged vulnerabilities in network segmentation that enabled the perpetrators to conduct the attack but stopped short of attributing the attack to a non-state actor or a nation state.

## State Practice

While India has taken a clear stance to not publicly attribute, others have taken a different route. A number of countries have expressed national positions on attribution, either in statements on the applicability of international law to cyberspace or in their national cybersecurity strategies.[21] France,[22] Germany,[23] Finland,[24] and Italy[25] clearly state that the choice to publicly attribute or not is a national sovereign prerogative and an independent decision to be made by each nation-state. While all states refer to the applicability of the existing international law on cyber attribution to cyberspace, some underscore the relevance of the political aspects of cyber attribution. France and Finland explicitly state that the decision to attribute a cyberattack originating in another state is a national political decision that must take several circumstances and evidence into account.

The Netherlands has considered public attribution a cornerstone of cyber defence. In their latest Cyber Defense Strategy, it argues: "An active political attribution policy contributes to the deterrent ability and makes the Netherlands less attractive as a target of cyberattacks. A state actor who is held accountable for his actions will make a different assessment than an attacker who can operate in complete anonymity."[26] The 2015 United States Department of Defense's Cyber Strategy further acknowledges the role of attribution in establishing a credible cyber deterrence strategy and articulates the US's cyber attribution capacity "on matters of intelligence, attribution, and warning, DoD and the intelligence community have invested significantly in all source collection, analysis, and dissemination capabilities, all of which reduce the anonymity of state and non-state actor activity in cyberspace."[27]

State-led public attributions for cyberattacks thus far have mostly been carried out by the US, the EU, and their NATO partners.[28] With notable exceptions such as Brazil and Pakistan, these are the same states that have weighed in officially on the applicability of existing international law standards to cyberspace.

Other states, such as China, are more circumspect about the public attribution of cyberattacks by the US and its partners in the Five Eyes intelligence alliance (Australia, Canada, New Zealand, and the UK).[29] In Beijing's view, public attributions by the US are underscored by vague norms regarding the acceptable limits of offensive cyber operations and act as both a legal weapon to legitimise future indictments and sanctions against China and a political weapon to inflict

reputational costs on the adversary.[30] This position need not be taken at face value, though. Beijing itself participates in offensive cyber activity, and the claim of politicisation itself could be used to delegitimise US attribution and follow-up action, even if they are in line with accepted standards of international law.

## International Legal Standards

The international law on attribution for the purpose of affixing state responsibility is relatively well-settled, although its application to specific contexts, including in the cyber realm, remains a challenge. As per international law, state responsibility is premised on two components: an act or omission that amounts to the breach of an international obligation, and an attribution of said act or omission to a state in question. The acts of a private person are not attributable to a state unless the private actor is within the "effective control" of the state; that is, it is "in fact acting on the instructions of, or under the direction or control of that State in carrying out the conduct."[31]

The law of state responsibility does not, however, weigh in on evidentiary standards or burdens of proof. Further, there is no international legal obligation to provide evidence backing up a public attribution.[32] Standards of "sufficient levels of confidence"[33] or "sufficient certainty"[34] have been proposed to assess evidence before a decision to publicly attribute is made.

## Global Forums

Global forums fermenting responsible state behaviour in cyberspace have recognised the relevance of attribution to these debates. The 2015 consensus report of the United Nations Group of Governmental Experts (UN-GGE), set up to identify norms for responsible state behaviour in cyberspace, suggested a norm on cyberattack attribution.[35] Norm 13 (b) reads: "In the case of ICT incidents, States should consider all relevant information including the larger context of the event, the challenges of attribution in the ICT context, and the nature and extent of the consequences." The 2021 UN-GGE report provided further guidance on aspects that states may consider in the decision-making process, such as the technical attributes of the attack, scope, scale and impact, consultations between the states, and the wider contextual implications on international peace and security.[36]

The 2021 report also recommended cooperation between Computer Emergency Response Teams that could improve state capacity in detecting and investigating malicious attacks. Finally, it recommended that states proactively use regional, bilateral, and multilateral forums to exchange best practices and cast light on national approaches to attribution, with the overarching goal of fostering common understandings and an exchange of best practices.

## Private Sector Attribution

It is also worth noting that several public attributions have been conducted by private sector actors. Cybersecurity firms Mandiant[37] and Crowdstrike[38] have published detailed reports attributing high-profile cyber incidents to China and Russia, respectively. Recorded Future, another US-based cybersecurity firm, has attributed the continuous targeting of critical infrastructure in India, including electricity grids, to Chinese state-sponsored groups.[39] With the ongoing armed conflict in Ukraine, US-based technology companies such as Microsoft and Google have published detailed blog posts publicly attributing aggressive, offensive cyber activity to Russian-backed cyber actors looking to gain decisive war-time advantage. Non-government organisations such as Citizen Lab,[40] Electronic Frontier Foundation,[41] and Amnesty International[42] have also publicly attributed the deployment of offensive cyber capabilities, largely in instances where these capabilities have been deployed against journalists, politicians, or human rights defenders.

Given their role in the growing ecosystem of "decentralised cyber attribution",[43] these private actors have also weighed in on the necessary methods, processes, and evidentiary considerations for public attribution. For example, in a detailed blog post, 'Navigating the trade-offs of cyber attribution,' Mandiant researchers highlight four trade-offs for security leaders when making the decision to publicly attribute.[44] These include the allocation of resources, the trade-off between analytical independence and neglecting important insights from other actors also involved in the attribution processes, between making rash attribution judgments that risk misattribution and an overly cautious approach that prevents the detection and necessary action regarding a cyberattack, and, finally, the decision to go public itself. On going public, Mandiant recommends considering several factors, including source sensitivities, a victim's reaction, the impact on the attacker's geopolitical context, and implications for ongoing cyber engagements. Compared to the broader guidelines articulated in the 2021 UN-GGE report, Mandiant offers more specific guidance which may be operationally useful for decision-makers.

# A Decision-Making Framework

The decision-making framework for publicly attributing cyber incidents should appreciate the multiple possible goals of cyber attribution, utilise India's institutional architecture effectively, and have clear criteria in place at each step of the detection and attribution process. Most significantly, decision-makers must keep in mind that publicly attributing a cyberattack does not signal a cyber defence failure to the Indian public or the wider world.[45] Cyberattacks and breaches are an accepted part of today's geopolitical scenario. A well-articulated cyber attribution could signal that the Indian institutional architecture and forensic capability are resilient enough to deal with this new reality.

As articulated by Egloff and Smeets, public attribution could be considered by decision-makers looking to pursue one or more goals.[46] Drawing from their work, policymakers could consider the objectives discussed in the following paragraphs:

**Deterrence:** Public attribution could deter adversaries from carrying out future attacks as they fear getting caught and facing punitive measures. Most analysts, however, disagree with the deterrence potential of simply 'naming and shaming'. They argue that without follow-up action, such as sanctions, 'naming and shaming' may end up encouraging adversaries to continue their exploits. Even if followed up with sanctions, the costs imposed may not be significant enough to alter macro decision-making on continuing to undertake offensive cyber operations, given the gains to be made through espionage or other forms of offensive operations.[47] Further, as is the case with the India-Pakistan context, in several instances, cyber proxies may be operating at an arm's length from the state and have little to lose if sanctions or reputational costs are imposed on the state.

**Causing friction:** Publicly revealing evidence regarding an adversary's capabilities could serve counter-threat objectives as the adversary would need to develop new capabilities to avoid detection in the future. Friction does not prevent adversaries from mounting continuous action but imposes operational hurdles.

**Building resilience across the ecosystem:** Public attribution and disclosure of evidence on capabilities and vulnerabilities could help network owners both in the public and private sectors to audit and secure their own hardware and software systems accordingly.

**Norm-building:** 'Naming and shaming' action that violates norms agreed upon at international forums strengthens the norm by "demarcating what is appropriate behaviour" and publicly pushing countries to comply. Of course, norm-building works best if norms of responsible state behaviour or prevailing understandings of international law are explicitly referenced in the statement attributing specific cyber incidents.

**Community and international cooperation:** Attribution published to the general public or shared with trusted partners in the research community, or the Computer Emergency Response Teams (CERTs) could jointly strengthen attribution capabilities and aid in detecting cyber threats. Further, such information-sharing mechanisms could help build international credibility and confidence among partners in plurilateral mechanisms such as the Quadrilateral Security Dialogue.

**Domestic criminal law enforcement:** With enough forensic evidence to justify violating domestic criminal law, states may publicly attribute a cyberattack through an indictment before the judiciary. The US Department of Justice, for instance, announced indictments against 41 criminal actors based in Russia, China, Iran and North Korea[48] and also indicted officers of the Russian Main Intelligence Directorate Unit in 2020.[49]

## Institutional Architecture and Decision-Making Framework on Cyber Attribution

A number of agencies within India's institutional architecture for cybersecurity should play a coordinated role in the proposed cyber attribution model. This includes the Prime Minister's Office comprising the technical intelligence agency National Technical Research Organization and the National Critical Information Infrastructure Protection Centre (NCIIPC).[50] India's computer emergency response team falls within the jurisdiction of the Ministry of Electronics and Information Technology and is responsible for detecting, mitigating, and preventing cybersecurity incidents. Finally, there is the Defence Cyber Agency, first announced in 2018, which draws armed forces personnel from all three branches and falls within the Ministry of Défense.

A cyber incident would generally be detected by CERT-In or the NCIIPC in the case of critical infrastructure. After the forensic characterisation, decision-makers may choose to go public based on several factors, including the level

of confidence in the characterisation; the need to protect sensitive sources; geopolitical considerations such as whether the attack originates from an adversarial or friendly country; available response options that could be undermined by a public attribution; the severity of the attack; and risks of escalation.[51]

If the decision to go public is made, the attribution format is equally important. Policymakers could consider one of four options.[52]

**Option A: Criminal Indictment**

The first option is a criminal indictment that can be exercised if the law enforcement authorities have sufficient evidence to prosecute under the Indian Penal Code or Information Technology Act. As we are dealing with international cyber incidents, the chargesheet of a First Information Report should be filed by a central investigative agency.

Effort should be made to ensure that this indictment makes it way independently through the legal system. While it is likely that the perpetrators will never end up in court, this option helps establish credibility[53] in the public attribution through the rigour required by the domestic legal system. Further, any links the perpetrators have with individuals or entities within Indian jurisdiction can be legitimately sanctioned within the purview of Indian domestic law. This option works when attributing attacks to non-state actors, and by itself will not enable attribution to state actors.

**Option B: International legal attribution**

The second option is international legal attribution to a state as per the evidentiary standards of international law including, most importantly, the Law of State Responsibility. International legal attribution is important if India is considering cyber or kinetic countermeasures to the cyberattacks that may need to be justified domestically or internationally. The attribution statement should be released by the office of the National Cybersecurity Coordinator, either jointly or in close consultation with the Ministry of External Affairs and relevant legal experts, either working full-time in the Ministry or as consultants.

Before effectively attributing specific cyber incidents, India must issue a statement clearly highlighting the Indian perspective on how international law applies to cyber attribution and the necessary evidentiary standards. Without such understanding, the legitimacy and credibility of each specific cyber attribution may be questioned as being politically motivated and lacking consistency.

**Option C: Political attribution**

The third option is a political attribution at the Ministerial level that need not reference international law or meet evidentiary standards. Instead, the goal is to win "the hearts and minds of audiences that open up with public attribution."[54] Indeed, most public cyber attributions have not referenced domestic or international law.[55]

Indian politicians often politically attribute cross-border terrorism to geopolitical adversaries like Pakistan without referencing legal standards.[56] This is done to strengthen India's position on sanctioning individuals associated with terrorism at multilateral processes; nudging Pakistani authorities to address the issue through their domestic capacity; ferment global laws and norms against terrorism; or score political points with a domestic audience. The same approach may be applied to cyberattacks where evidence points in a certain direction and a political attribution is likely to aid Indian objectives without sparking escalation from the country at the receiving end of the attribution.

**Option D: Do nothing and rely on third-party attribution**

A fourth option is to rely on third-party attribution. As discussed earlier, the private sector and civil society have been doing an effective job of publicly attributing cyberattacks as well as crafting their own policy and strategies on the same. A potential option here for the Indian government in cases where an initial attribution has been done by a private actor such as Mandiant or Recorded Future could be to "acknowledge" the report but neither confirm nor deny its findings.

To be sure, this option may have similar consequences as the decision to not attribute in the first place. However, the trade-offs, outcomes, and decision-making processes are entirely different. In a case where India decides to not publicly attribute at all and there is no evidence from a third-party actor, India

has to live with the possibility that the attack may not get attributed at all. Option D outlines the trade-offs involved in situations where a public attribution has been conducted or is in the process of being conducted by a third-party organisation, which means that the attack will be publicly attributed, just not by the Indian government.

## Table 1: Options for Public Attribution for India

| Option | When to use | Who should attribute |
|---|---|---|
| Criminal indictment | 1. Attribution only to a private actor.<br>2. Evidentiary thresholds meet the requirement of domestic Indian law. | Central or state criminal investigative agency |
| International Law Attribution | 1. Attribution to a state actor.<br>2. Evidence satisfies international law thresholds.<br>3. Potentially useful if public countermeasures are being considered. | National Cyber Security Coordinator and Ministry of External Affairs |
| Political attribution | When evidence may not be sufficient for legal attribution but attribution may further India's geopolitical calculations or interests at global forums. | Political officials (ideally, Cabinet Level Ministers) |
| Do nothing and rely on third party attribution | Insufficient evidence to publicly attribute or attributing poses risks. | Joint decision could be taken by NCSC or acknowledgment of private attribution |

*Source: Author's own*

# Conclusion

None of these available options, either individually or in concert, will necessarily achieve the set-out goals given the variables at play. However, bearing this framework in mind provides decision-makers with more options. For example, a criminal indictment underscored by a strong public statement by the National Cyber Security Coordinator could demonstrate India's capabilities while undermining that of adversaries even if no one faces a single day in court.

To implement a model and attribute both effectively and responsibly, India must create coordination mechanisms that bring all relevant government and non-government entities into the decision-making spectrum. CERT-In should certainly be involved with any such process given their role and existing capacity, but sector-specific stakeholders and government entities must also play their part.

Effective characterisation of a cyber incident and consequent public attribution can be furthered by regularly discussing methodological challenges, and opportunities, and sharing intelligence with trusted partners such as the Quadrilateral Security Dialogue, which already has avenues for exchanges between the top cybersecurity personnel of the member countries, and has also envisaged greater cooperation between the respective CERTs. While sharing threat intelligence is easier among formalised military alliances, there is enough trust between Quad partners in the security and technological domains to create appropriate processes and mechanisms.

Given its geopolitical position in cyberspace, India cannot afford to not use the critical option of public attribution, when deemed effective, to navigate the uncertainty of cyber unpeace and further its strategic interests. Cyber unpeace is here to stay and cannot be wished away; the imperative is to use institutions, norms, and capabilities to mitigate its impact.

*The first version of this brief appeared in the ORF-GP volume,* Future Warfare and Critical Technologies: Evolving Tactics and Strategies, *which can be accessed here: https://www.orfonline.org/public/uploads/posts/pdf/20240212113627.pdf*

**Arindrajit Basu** *is a PHD Candidate at the Leiden University Faculty of Global Governance and Affairs.*

# Endnotes

1 Lucas Kello, *The Virtual Weapon and International Order* (New Haven, CT: Yale University Press, 2017), 78.

2 Lucas Kello, "Cyber Legalism: Why it Fails and What to Do About it," *Journal of Cybersecurity* 7, 2021, https://academic.oup.com/cybersecurity/article/7/1/tyab014/6343244.

3 David D. Clark and Susan Landau, "Untangling Attribution," in *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for US Policy*, ed. Committee on Deterring Cyberattacks (Washington, DC: The National Academies Press 2010), 25–40.

4 Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies* 38 (2015).

5 Clark and Landau, "Untangling Attribution"

6 Rid and Buchanan, "Attributing Cyber Attacks"

7 John S. Davis II et al., *Stateless Attribution: Toward International Accountability in Cyberspace* (Santa Monica: RAND Corporation, 2017).

8 Izumi Nakamitsu, "Remarks at the UN Securiry Council Open Debate on Cyber Security: Maintaining International Peace and Security in Cyberspace" (speech, VTC, June 29, 2021), UNODA, https://un.mfa.ee/wp-content/uploads/sites/57/2021/06/Nakamitsu-29-June.pdf.

9 Florian J. Egloff and Max Smeets, "Publicly Attributing Cyber Attacks," *Journal of Strategic Studies* 46, no. 3 (2023), https://www.tandfonline.com/doi/full/10.1080/01402390.2021.1895117; Ariel (Eli) Levite and June Lee, "Attribution and Characterization of Cyber Attacks," in *Managing U.S.-China Tensions Over Public Cyber Attribution*, ed. Ariel E. Levite et al. (Washington DC: Carnegie Endowment for International Peace, 2023), https://carnegieendowment.org/2022/03/28/attribution-and-characterization-of-cyber-attacks-pub-86698; Dennis Broeders, Els De Busser, and Patryk Pawlak, "Three Tales of Attribution in Cyberspace: Criminal Law, International Law and Policy Debates," The Hague Program for Cyber Norms, 2020, https://www.universiteitleiden.nl/en/research/research-output/governance-and-global-affairs/three-tales-of-attribution-in-cyberspace.-criminal-law-international-law-and-policy-debates.

10 Rajeswari Pillai Rajagopalan and Sameer Patil, "Introduction" in Rajeswari Pillai Rajagopalan and Sameer Patil (eds)*Future Warfare and Critical Technologies: Evolving Tactics and* Strategies (Observer Research Foundation,2024)

11 K. V. Kurmanath, "India Emerges as Top-3 Target for Nation-State Driven Cyber Attacks," *Business Line*, October 6, 2023, https://www.thehindubusinessline.com/info-tech/india-emerges-as-top-3-target-for-nation-state-driven-cyber-attacks/article67387522.ece

12 Tech Desk, "Cyber Attacks Increased by 18 Per Cent This Year Alone in India," *Indian Express*, May 7, 2023, https://indianexpress.com/article/technology/tech-news-technology/cyber-attacks-in-india-increased-by-18-per-cent-in-2023-check-point-8596348/.

# Endnotes

13 See for a detailed coverage of notable cyber incidents, Sameer Patil, *Securing India in the Cyber Era* (Oxon: Routledge,2022).

14 Express News Service, "Cosmos Bank Malware Attack: Pune Court Convicts 11 Accused," *Indian Express*, April 23, 2023, https://indianexpress.com/article/cities/pune/cosmos-bank-malware-attack-pune-court-convicts-11-accused-8570830/.

15 Melissa Robbins, "Cyberattack Hits Indian Nuclear Plant," *Arms Control Today*, December 2019, https://www.armscontrol.org/act/2019-12/news/cyberattack-hits-indian-nuclear-plant.

16 Ashish Aryan, "AIIMS Cyber Attack Took Place Due to Improper Networks Segmentation," *Economic Times*, February 10, 2023, https://economictimes.indiatimes.com/tech/technology/aiims-cyber-attack-took-place-due-to-improper-network-segmentation-govt-in-rs/articleshow/97805598.cms?from=mdr.

17 Soumik Ghosh, "Lack of Cyber Attribution a Major Challenge for India: Lt. Gen Pant," CSO, September 2, 2020, https://www.csoonline.com/article/569797/lack-of-cyber-attribution-a-major-challenge-for-india-lt-gen-pant.html.

18 Mahender Singh Manral, "35 Percent of Cyber Attacks on Indian Sites from China: Official Report," *Indian Express*, August 23, 2018, https://indianexpress.com/article/india/35-of-cyber-attacks-on-indian-sites-from-china-official-report/.

19 ANI, "'Human Error, Not Chinese Cyber Attack,' Says Union Power Minister on Mumbai 2020 Blackout," *Economic Times*, May 3, 2021, https://energy.economictimes.indiatimes.com/news/power/human-error-not-chinese-cyber-attack-says-union-power-minister-on-mumbai-2020-blackout/81303209

20 Aryan, "AIIMS Cyber Attack Took Place Due to Improper Networks Segmentation"

21 NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), "Attribution," in *NATO CCDCOE Excellence Cyber Law Toolkit Database*, https://cyberlaw.ccdcoe.org/wiki/Attribution; NATO CCDCOE Cyber Law Toolkit, https://cyberlaw.ccdcoe.org/wiki/Main_Page.

22 Ministry of Defense of France, International Law Applied to Operations in Cyberspace, September 9, 2019.

23 Federal Government of Germany, "On the Application of International Law in Cyberspace," 2021, https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf.

24 Ministry of Foreign Affairs, "Finland Published its Positions on Public International Law in Cyberspace," Finnish Government, October 15, 2020, https://valtioneuvosto.fi/en/-/finland-published-its-positions-on-public-international-law-in-cyberspace.

25 Italian Ministry for Foreign Affairs and International Cooperation, "Italian Position Paper on International Law and Cyberspace," 2021, https://www.esteri.it/mae/resource/doc/2021/11/italian_position_paper_on_international_law_and_cyberspace.pdf.

# Endnotes

26 Ministerie van Defensie, "Defensie Cyber Strategie 2018: Investeren in Digitale Slagkracht Voor Nederland," trans. Egloff and Smeets, 2018.

27 The Department of Defense, *The Department of Defense Cyber Strategy* (Washington DC: Department of Defense), https://www.hsdl.org/c/view?docid=764848.

28 Lu Chuanying, "A Chinese Perspective on Cyber Attribution," in *U.S.-China Tensions over Public Cyber Attribution*, ed. Ariel E. Levite et al., (Washington DC: Carnegie Endowment for International Peace, 2023)

29 Chuanying, "A Chinese Perspective on Cyber Attacks"

30 Levite and Lee, "Attribution and Characterization of Cyber Attacks"

31 International Law Commission, "Responsibility of States for Internationally Wrongful Acts 2001," United Nations, https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf; Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017), Rule 17.

32 NATO CCDCOE, "Attribution"

33 Federal Government of Germany, "On the Application of International Law in Cyberspace"

34 NATO CCDCOE, "National Position of the Netherlands (2019) in the NATO CCDCOE Cyber Law Toolkit Database," https://cyberlaw.ccdcoe.org/wiki/National_position_of_the_Netherlands_(2019); NATO CCDCOE Cyber Law Toolkit, https://cyberlaw.ccdcoe.org/wiki/Main_Page.

35 "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," July 22, 2015, https://digitallibrary.un.org/record/799853?ln=en.

36 "Group of Governmental Experts in the Field of Information and Telecommunications in the Context of International Security," July 14, 2021, https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf.

37 "APT1: Exposing One of China's Espionage Units," *Mandiant*, December 30, 2021, https://www.mandiant.com/resources/reports/apt1-exposing-one-chinas-cyber-espionage-units.

38 Brian Ross et al., "'Beyond a Reasonable Doubt' Russians Hacked DNC, Analyst Says," *abc News*, July 26, 2016, https://abcnews.go.com/International/reasonable-doubt-russians-hacked-dnc-analyst/story?id=40863292.

39 INSIKT Group, "Continued Targeting of Indian Power Grid Assets by Chinese State-Sponsored Activity Groups," *Recorded Future*, April 6, 2022, https://www.recordedfuture.com/continued-targeting-of-indian-power-grid-assets.

40 "NSO Group," The Citizen Lab, https://citizenlab.ca/tag/nso-group/.

# Endnotes

41 Cooper Quintin and Eva Galperin, "Dark Caracal: You Missed a Spot," Electronic Frontier Foundation, December 10, 2020, https://www.eff.org/deeplinks/2020/12/dark-caracal-you-missed-spot.

42 Amnesty International, "The Pegasus Project: How Amnesty Tech Uncovered the Spyware Scandal-New Video," Amnesty International, March 23, 2022, https://www.amnesty.org/en/latest/news/2022/03/the-pegasus-project-how-amnesty-tech-uncovered-the-spyware-scandal-new-video/https://www.amnesty.org/en/latest/news/2022/03/the-pegasus-project-how-amnesty-tech-uncovered-the-spyware-scandal-new-video/.

43 Kristen. E. Eichensehr, "Decentralized Cyber Attack Attribution," AJIL Unbound, June 24, 2019, https://www.cambridge.org/core/journals/american-journal-of-international-law/article/decentralized-cyberattack-attribution/36189FEEC7937C0588C1A782BDBB4395.

44 Jamie Collier and Shanyn Ronis, "Navigating the Trade-Offs of Cyber Attribution," *Mandiant*, January 17, 2023, https://www.mandiant.com/resources/blog/trade-offs-attribution#:~:text=Attribution%20percent20matters%20percent2C%20percent20but%20percent20to%20percent20what,regularly%20percent20involves%20percent20difficult%20percent20trade%20percent2Doffs.

45 Sameer Patil (discussion with author, October 18, 2023).

46 Egloff and Smeets, "Publicly Attributing Cyber Attacks"

47 Jack Goldsmith and Robert D. Williams, "The Failure of the United States' Chinese-Hacking Indictment Strategy," *Lawfare*, December 28, 2018, https://www.lawfareblog.com/failure-united-states-chinese-hacking-indictment-strategy.

48 Garrett Hinck and Tim Maurer, "Persistent Enforcement: Criminal Charges as a Response to Nation-State Malicious Cyber Activity," *Journal of National Security Law and Policy* 10 (2020): 528.

49 Department of Justice, Government of the United States, https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and.

50 For details on India's cybersecurity architecture, see Arindrajit Basu, *India's International Cyber Operations: Tracing National Doctrine and Capabilities*, United Nations Institute for Disarmament Research, Geneva, UNIDIR, 2022, https://www.unidir.org/cyberdoctrines/India.

51 Levite and Lee," "Attribution and Characterization of Cyber Attacks""

52 See Broeders, De Busser and Pawlak for a good overview of various options

53 Arindrajit Basu, "Lessons from US response to cyber attacks," Hindu Business Line,October 30,2018, https://www.thehindubusinessline.com/opinion/lessons-from-us-response-to-cyber-attacks-ep/article25372326.ece

54 Broeders, De Busser, and Pawlak, "Three Tales of Attribution in Cyberspace"

# Endnotes


55 Dan Efrony and Yuval Shany, "A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice," *American Journal of International Law* 112, no. 4 (2018), https://www.cambridge.org/core/journals/american-journal-of-international-law/article/abs/rule-book-on-the-shelf-tallinn-manual-20-on-cyberoperations-and-subsequent-state-practice/54FBA2B30081B53353B5D2F06F778C14.

56 India Today News Desk,"'Terrorism by night,trade by day': S Jaishankar rips into Pakistan," India Today,Jun 29,2023,https://www.indiatoday.in/india/story/eam-jaishankar-saarc-pakistan-cross-border-terrorism-india-china-ladakh-standoff-khalistan-issue-2399391-2023-06-29


*Images used in this paper are from Getty Images/Busà Photography.*

ORF OBSERVER RESEARCH FOUNDATION

**Ideas . Forums . Leadership . Impact**

**20, Rouse Avenue Institutional Area,**
**New Delhi - 110 002, INDIA**
**Ph. :** +91-11-35332000. **Fax :** +91-11-35332005
**E-mail:** contactus@orfonline.org
**Website:** www.orfonline.org