GCSP
Geneva Centre for Security Policy

The Attribution of Cyber Operations to States in International Law

Hui Chen, Antonio Coco, Annachiara Rotondo, and Yaohui Ying

Sino-European Expert Working Group on the Application of International Law in Cyberspace (EWG-IL), Research Group Report 2025. A joint research initiative between the GCSP and the China Institutes of Contemporary International Relations, EU Cyber Direct, Xiamen University and Suzhou Academy of Xi'an Jiaotong University.

Geneva Centre for Security Policy
Maison de la paix
Chemin Eugène-Rigot 2D
P.O. Box 1295
1211 Geneva 1
Switzerland
Tel: + 41 22 730 96 00
Contact: www.gcsp.ch/contact
www.gcsp.ch

ISBN: 978-2-88947-034-1

About the partner organisations

CICIR
中国现代国际关系研究院
CHINA INSTITUTES OF CONTEMPORARY INTERNATIONAL RELATIONS

The China Institutes of Contemporary International Relations (CICIR) is a long-standing, extensive, and multifunctional research and consultation complex focusing on international strategic and security studies. It covers all geographic areas and major global strategic and comprehensive issues. The CICIR has about 300 staff, including researchers and administrative and logistical personnel, who work for 15 institutes, a number of centres, and several offices. For years it has participated in wide-ranging, comprehensive and high-end international academic exchanges. The CICIR is authorised to confer master's and doctoral degrees, and publishes three academic journals: *Xiandai Guoji Guanxi, Contemporary International Relations* and *China Security Studies.*

EU CYBER DIRECT

EU Cyber Direct – EU Cyber Diplomacy Initiative supports the European Union's cyber diplomacy and international digital engagements in order to strengthen a rules-based order in cyberspace and build cyber-resilient societies. To fulfil this aim it conducts research, supports capacity-building in partner countries and promotes multistakeholder cooperation. Through research and events, EU Cyber Direct regularly engages in discussions about the future of international cooperation to fight cybercrime and strengthen criminal justice systems globally.

GCSP
Geneva Centre for Security Policy

The Geneva Centre for Security Policy (GCSP) is an international foundation that aims to advance global cooperation, security, and peace. Governed by 55 Member States, this flagship foundation is supported by the Swiss government to provide a unique 360° approach to learn about and solve global challenges. Our mission is to educate leaders, facilitate dialogue, advise through in-house research, inspire new ideas and connect experts to develop sustainable solutions for a more peaceful future.

厦門大學

Xiamen University (XMU), established in 1921, has long been listed among China's leading universities on the national 211 Project, 985 Project, and Double First-Class Initiative, which were launched by the Chinese government to support selected universities in achieving world-class standing. With a graduate school, six academic divisions consisting of 35 schools and colleges, and 17 research institutes, XMU boasts a total enrolment of nearly 47,000 full-time students and has over 3,000 full-time teachers and researchers, 15 of whom are members of either the Chinese Academy of Sciences or the Chinese Academy of Engineering.

西安交通大學 苏州研究院
XI'AN JIAOTONG UNIVERSITY SUZHOU ACADEMY

Founded in May 2004, Xi'an Jiaotong University Suzhou Academy is a legal-person scientific research unit under Xi'an Jiaotong University and also undertakes management functions. The core mission is to build four key bases in Suzhou for Sino-foreign cooperative education, education and training, scientific research, and the transformation of scientific and technological achievements. Supporting the local social and economic development is one of its important tasks.

Background

This report has been produced in the context of a larger research and dialogue project, in terms of which the China Institutes of Contemporary International Relations, EU Cyber Direct, the Geneva Centre for Security Policy, and Xiamen University and Suzhou Academy of Xi'an Jiaotong University, convene a joint Sino-European Expert Working Group on the Application of International Law in Cyberspace (EWG-IL). The working group provides a platform for exchange among European and Chinese legal experts to examine the application of international law in cyberspace and to examine related problems from a theoretically legal perspective. The main goal of the work in research groups is to provide more thorough analysis of the selected topics and identify points of divergence and convergence between Europe and China with the aim of creating a more evidence-based and trusted environment for policy discussions in Track 1.5. and Track 1 processes.

Authors

Chinese team:

Dr Hui CHEN, Assistant Researcher, Institute of Cyberspace Governance of Wuhan University

Dr Yaohui YING, Assistant Professor, School of Law, Zhongnan University of Economics and Law

European team:

Dr Antonio COCO, Associate Professor, Essex Law School, University of Essex

Dr Annachiara ROTONDO, Assistant Professor, Università degli Studi di Napoli Federico II

Acknowledgement

This report was sponsored by the Swiss Federal Department of Foreign Affairs, whose generous support is greatly appreciated. The constructive feedback and valuable insights of the reviewers, Mr Kubo Mačák and Prof. Hua Zhang, whose expertise has contributed to the quality of this publication, are also gratefully acknowledged.

Contents

1. Applicable law and preliminary questions

1.1 Types of attribution in the cyber domain

The term "attribution" refers to the process of identifying the actor responsible for a particular type of conduct (action or omission). Three distinct yet interconnected forms of attribution can be identified: technical, political and legal. While each has a different function and evidentiary base, it is legal attribution that carries normative weight in the framework of international responsibility as one of the requirements for the existence of an internationally wrongful act.[1]

In this respect, legal attribution refers to the process of imputing a given action or omission carried out by organs, entities, individuals or groups (for this report, through the use of information and communication technologies) to a state, for the purposes of the law on international responsibility.[2] Legal attribution – which will be the exclusive focus of the present report – is governed by the rules reflected in the Articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA),[3] which for the most part is considered to reflect customary international law and is generally deemed to be applicable to cyber activities.[4]

By contrast, technical attribution focuses on identifying the factual parameters of a cyber operation – such as its origin, methods and infrastructure – using forensic tools. It serves as the evidentiary substrate upon which legal and political assessments are often constructed, but does not itself establish legal responsibility.[5]

Finally, political attribution consists of public or strategic declarations of responsibility, which are often grounded in intelligence or geopolitical assessments rather than formal legal standards. Importantly, political attribution cannot by itself serve as a legal basis for responses such as countermeasures under international law, because these responses require a prior internationally wrongful act attributable to a state under ARSIWA. In this sense, while political attribution may influence diplomatic or political responses, it lies outside the doctrinal structure of international law concerning state responsibility.

1.2 Legal basis of the rules of attribution

Articles 4-11 of ARSIWA, which set out the criteria under which the conduct of persons or entities may be attributed to a state, are widely recognised as reflecting customary international law.[6]

---

1 K. Eichensehr, "The Law & Politics of Cyberattack Attribution", *UCLA Law Review*, Vol.67, 2020, p. 520.

2 International Law Commission (ILC), "Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries", 2001, art 2, p. 36, para. 12.

3 Ibid., arts. 4-11.

4 Some states (New Zealand, Japan, Republic of Korea) emphasise that rules on the international responsibility of states for wrongful acts expressly find application in the context of cyber activities (OEWG (Open-Ended Working Group), "Compendium of Statements in Explanation of Position on the Final Report", A/AC.290/2021/INF/2, 25 March 2021, pp. 51, 60; OEWG, "Compendium of Statements in Explanation of Position on the Final Report", Addendum, A/AC.290/2021/INF/2/Add.2, 29 November 2021, p. 2).

5 N. Tsagourias and M. Farrell, "Cyber Attribution: Technical and Legal Approaches and Challenges", *European Journal of International Law*, Vol.31, 2020, p. 941.

6 A. Orakhelashvili, *Akehurst's Modern Introduction to International Law*, Routledge, 2019, p. 276; J. Crawford, *Brownlie's Principle of*

In practice, states routinely rely on ARSIWA when referring to responsibility in international legal disputes. For instance, in pleadings before international tribunals, states frequently cite specific attribution provisions to support their claims or defences.[7] This recurring invocation constitutes strong evidence and *opinio juris* and confirms that states treat these rules as legally binding. Moreover, international courts and tribunals – most notably the International Court of Justice (ICJ) – have repeatedly endorsed the legal authority of Articles 4-11 as customary international law.[8] In *Nicaragua v. the United States* (1986), the ICJ articulated the "effective control" standard for attributing the conduct of non-state actors to a state, in terms consistent with what became the text of Article 8 ARSIWA.[9] Finally, leading scholars in the field of international law have consistently affirmed the customary status of these provisions. James Crawford, the former Special Rapporteur for the International Law Commission (ILC) on State Responsibility, explicitly described Articles 4-11 ARSIWA as codifications of existing customary norms.[10] This position is widely echoed in major treatises and commentary,[11] where these articles are treated not as mere proposals, but as expressions of general international law.

Taken together, state practice, consistent judicial affirmation, and scholarly consensus establish that Articles 4-11ARSIWA mirror the rules of customary international law. As such, they provide the primary legal framework for questions of attribution for the purposes of international responsibility, including in the context of cyber operations. Of note, Article 55 ARSIWA acknowledges the possibility of special rules of international law (*lex specialis*) governing the conditions for the existence of an internationally wrongful act, potentially including specific rules of attribution; however, the existence of any such special rules in the cyber context remains contested.[12]

1.3 Legal challenges posed by cyber operations

Attributing cyber operations to a state presents a distinct set of legal challenges stemming from both the technical structure of cyberspace and the normative complexity of international responsibility. The inherent anonymity of the digital domain, the routine use of obfuscation techniques, and the involvement of proxy

Public International Law, Oxford University Press, 2019, p. 524; N. Tsagourias and R. Buchan (eds), *Research Handbook on International Law and Cyberspace*, Edward Elgar, 2021, p. 115; M.N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, 2017, p. 79.

7 UNGA (UN General Assembly), "Responsibility of States for Internationally Wrongful Acts: Compilation of Decisions of International Courts, Tribunals and Other Bodies", Addendum, A/71/80/Add.1, 20 June 2017, identifying 163 cases with 392 references to the State responsibility articles in publicly available decisions taken during the period from 1 January 2001 to 31 January 2016; UNGA, "Responsibility of States for Internationally Wrongful Acts: Compilation of Decisions of International Courts, Tribunals and Other Bodies", A/74/83, 23 April 2019, identifying 86 cases referring to ARSIWA; UNGA, "Responsibility of States for Internationally Wrongful Acts: Compilation of Decisions of International Courts, Tribunals and Other Bodies", A/77/74, 29 April 2022, identifying 83 decisions referring to ARSIWA; UNGA, "Responsibility of States for Internationally Wrongful Acts: Compilation of Decisions of International Courts, Tribunals and Other Bodies", A/80/77, 23 April 2025, identifying a further 88 decisions referring to ARSIWA.

8 E.g. Case Concerning Armed Activities on the Territory of the Congo (*DR Congo v. Uganda*), *ICJ Reports 2005*, p. 168, paras. 160, 293; Case Concerning the Application of the Convention on the Prevention and Punishment of the Crime of Genocide (*Bosnia and Herzegovina v. Serbia and Montenegro*), *ICJ Reports 2007*, p. 43, paras. 173, 385, 398, 401, 414, 431, 460; Case Concerning the Application of the Convention on the Prevention and Punishment of the Crime of Genocide (*Croatia v. Serbia*), ICJ Judgment of 3 February 2015, para. 104.

9 Military and Paramilitary Activities in and against Nicaragua (*Nicaragua v. the United States*), *ICJ Reports 1986*, paras. 116-117.

10 Crawford, 2019, p. 524.

11 P. Gaeta, J.E. Viñuales and S. Zappalá, *Cassese's International Law*, Oxford University Press, 2020, p. 248; F. Delerue, *Cyber Operations and International Law*, Cambridge University Press, 2020, pp. 112-113.

12 M. Milanović, "Special Rules of Attribution of Conduct in International Law", *International Law Studies*, Vol.96, 2020, p. 295.

actors – such as ideologically aligned hacker collectives or state-tolerated cyber militias – undermine the ability to establish a clear nexus between the conduct and a state. These obstacles complicate the application of the attribution criteria set forth in ARSIWA, particularly Articles 5 and 8.

In response to these attribution dilemmas, some scholars and practitioners argue that ascertaining who should be held responsible under international law may in certain cases require more than definitively identifying the individual perpetrators.[13] Furthermore, the increasing integration of artificial intelligence (AI) and automated systems into cyber operations introduces additional complexity. These technologies may operate with minimal or no direct human intervention, thereby obscuring the human agency traditionally required for the invocation of state responsibility.

1.4 Relevance beyond the establishment of state responsibility

Although attribution rules are principally designed to establish responsibility for internationally wrongful acts, their application in the cyber context extends beyond this function. Attribution plays a key role in determining the legality of countermeasures and self-defence measures that may be adopted in response to wrongful cyber activities. In addition, attribution may inform domestic regulatory responses, the formulation of cyber deterrence policy and the framing of normative expectations in global cyber governance.

13 J. Healey, "Beyond Attribution: Seeking National Responsibility for Cyber Attacks", Atlantic Council, 2012, http://www.jstor.org/stable/resrep03365.

2. Rules on the attribution of conduct to states

2.1 State organs in the context of cyber operations under Article 4 ARSIWA

The classification of a person or an entity as a "state organ" is a crucial step in the context of the attribution of cyber activities, because it serves as the primary legal basis under international law for linking the conduct of an individual or entity in the cyber context to the responsibility of a state.[14] The qualification of a person or entity as a state organ is to be inferred from the secondary rules on the international responsibility of states for wrongful acts, as reflected in ARSIWA, which are deemed to be applicable *vis-à-vis* the cyber domain.[15]

Under Article 4(1) ARSIWA, the term "state organ" encompasses any natural or legal person[16] integrated within the organisational structure of the state and acting in an official capacity,[17] irrespective of its function[18] and position in the state apparatus.[19] These subjects, commonly regarded as de jure organs,[20] are increasingly employed in cyber offensive/defensive operations such as those carried out by military cyber commands or equivalent bodies that are integrated within national armed forces (e.g. US Cyber Command, Russia's Main Directorate) or intelligence agencies involved in cyber surveillance, and are recognised as state organs by domestic law (e.g. US National Security Agency, UK Government Communications Headquarters).

However, under Article 4(2) ARSIWA, the qualification of a person or entity as a state organ does not rest solely on its designation under domestic law.[21] The determining factor is rather whether the individual/entity acts "in that capacity" as a de facto organ/agent, i.e. whether it performs functions of a public nature in "complete dependence" on the state, effectively functioning as a mere instrument of the state,[22] and carrying out its functions without any degree of operational autonomy. In the cyber context, this might hypothetically include a case where a state sets up a team comprising a private cybersecurity company and government

---

14 ILC, "Draft Articles", 2001, art. 4; ICJ, "Difference Relating to Immunity from Legal Process of a Special Rapporteur of the Commission on Human Rights", Advisory Opinion, *ICJ Reports 1999*, p. 62, para. 62.

15 Some states (New Zealand, Japan, Republic of Korea) emphasise that rules on the international responsibility of state for wrongful acts expressly find application in the context of cyber activities (OEWG, "Compendium of Statements in Explanation of Position on the Final Report", A/AC.290/2021/INF/2, 25 March 2021, pp. 51, 60; OEWG, "Compendium of Statements in Explanation of Position on the Final Report", Addendum, A/AC.290/2021/INF/2/Add.2, 29 November 2021, p. 2).

16 ILC, "Draft Articles", 2001, art. 4, para. 12.

17 J. Crawford, *State Responsibility: The General Part*, Cambridge University Press, 2013, p. 117.

18 ILC, "Draft Articles", 2001, art. 4, para. 6; C. Finkelstein, "Changing Notions of State Agency in International Law: The Case of Paul Touvier", *Texas International Law Journal*, Vol.30, 1995, pp. 261, 276-282; D.D. Caron, "The Basis of Responsibility: Attribution and Other Transsubstantive Rules of State Responsibility", in R.B. Lillich, D.B. Magraw and D.J. Bederman (eds), *The Iran United States Claims Tribunal: Its Contribution to the Law of State Responsibility*, Brill & Martinus Nijhoff, 1998, pp. 129-130.

19 ILC, "Draft Articles", 2001, art. 4, paras. 6-9.

20 C. Antonopoulos, "State Responsibility in Cyberspace", in N. Tsagourias and R. Buchan (eds), *Research Handbook on International Law and Cyberspace*, Edward Elgar, 2023, p. 116.

21 ILC, "Draft Articles", 2001, art. 4, para. 11; ICJ, *Application of the Genocide Convention* (*Bosnia and Herzegovina v. Serbia and Montenegro*), Judgment, 2007, paras. 385-395.

22 Ibid., para. 392; ICJ, Military and Paramilitary Activities in and against Nicaragua (*Nicaragua v. United States of America*), Merits, Judgment, *ICJ Reports 1986*, p. 14, paras. 109-110.

institutions for managing a cyber emergency, while retaining full authority over the team's activities. In this case, the team could be considered a state organ for the purposes of state responsibility, even if it lacks formal recognition or authorisation under national law.[23]

According to Article 7 ARSIWA, state (de jure and de facto) organs acting *ultra vires* – i.e. beyond legal authority or in violation of internal instructions – do not lose their legal status, and their conduct remains attributable to the state as long as it is carried out in an official capacity; e.g. in the case of a military cyber officer who disables another state's power grid using official infrastructure without authorisation. This provision, which is aimed at preventing states from evading responsibility solely on the basis that their organs or agents acted *ultra vires* or contrary to instructions, reflects a core principle of international responsibility: what matters is not the internal legality of the conduct, but the official capacity in which the act is performed.[24] By contrast, the conduct of individuals or entities who possess an official status but act in a personal capacity, e.g. accessing cyber infrastructure for criminal activity exclusively for private gain, is not attributable to the state under Article 4.[25]

2.2 The exercise of governmental authority by non-state actors with respect to activity in the cyber context

When cyber operations are carried out by actors operating outside the formal structure of the state – which is the most common case – the question arises as to whether and under what conditions their conduct can nevertheless be attributed to the state. Article 5 ARSIWA specifically addresses this scenario by establishing that actions or omissions performed by a person or entity that is not state organ but is empowered by domestic law to exercise elements of governmental authority shall be considered acts of the state if they are performed in that capacity, even when such persons/entities exceed their authority or contravene instructions.[26]

These actors may also fall within the category of de facto organs, but the threshold condition for attribution under this rule is not the same as Article 4(2) ARSIWA. Indeed, Article 5 asks for three indispensable and cumulative criteria: the conferral of public authority, the exercise of governmental authority, and that the person or entity acted in its official capacity.

The first requirement is satisfied when a person or entity is empowered by the law of the state to carry out functions that, by their nature, are normally associated with sovereign power. Hence, what matters is not the formal status of the actor, but rather the nature and source of its authority,[27] which is to be

23 K. Mačák, "Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors", *Journal of Conflict and Security Law*, Vol.21, 2016, p. 420.

24 ILC, "Draft Articles", 2001, Commentary to Article 7, paras. 1-4. See also ICJ, *"Difference Relating to Immunity from Legal Process of a Special Rapporteur of the Commission on Human Rights"*, Advisory Opinion, 1999, para. 62.

25 Schmitt, 2017, p. 89, para. 7.

26 ILC, "Draft Articles", 2001, art. 7, para. 1.

27 Ibid., art. 5, para. 3; D. Momtaz, "Attribution of Conduct to the State: State Organs and Entities Empowered to Exercise Elements of Governmental Authority", in J. Crawford et al. (eds), *The Law of International Responsibility*, Oxford University Press, 2010, pp. 244-246; Crawford, 2013, pp. 126-132.

granted explicitly in accordance with domestic law (e.g. through a law, executive order, statute, contract, etc.).[28] In the context of cyberspace, these entities can be private cybersecurity firms contracted for national cyber defence or internet service providers required by law to carry out surveillance.[29]

Under the second requirement, persons or entities must carry out actions that constitute, or are closely linked to, the exercise of governmental authority.[30] Since the exact contours of what constitutes "governmental authority" remain unsettled in international law,[31] it seems worth focusing on the classical distinction between acts carried out by a state in its sovereign capacity (*acta jure imperii*) and those undertaken in a commercial or private context (*acta jure gestionis*).[32] While this dichotomy is not always clear-cut in practice, the attribution of conduct under Article 5 ARSIWA presupposes that the private entity is acting within the framework of authority that reflects the sovereign prerogatives of the state.[33]

The third requirement assumes that a person or entity is acting in an official (and not a personal) capacity, which means that the individual or entity is performing functions on behalf of the state, as part of its assigned governmental role or authority: e.g. a government-employed intelligence officer carries out a cyber intrusion into a foreign country's electrical grid as part of a state-sponsored operation aimed at disabling critical infrastructure during a conflict. In contrast, acting in a personal capacity means that the person is acting for private purposes, not as a representative of the state, and therefore the conduct is not attributable to the state under international law.[34] Exceeding authority and violating instructions are not decisive factors when determining whether a person or entity empowered to exercise governmental authority *is acting in that capacity*.[35] The latter remains linked to the two key objective factors already discussed above: the legal or institutional link between the individual/entity and the state (e.g. public appointment, formal delegation, statutory mandate); and the nature and context of the act, specifically whether it was performed under the appearance of exercising public functions, regardless of whether the conduct breached internal rules.[36] As with the conduct of state organs, the conduct of a person or entity empowered to exercise elements of governmental authority is attributed

---

28 ILC, "Draft Articles", 2001, art. 5, para. 7. International jurisprudence supports this functional reading. In *Jan de Nul v. Egypt*, the International Centre for Settlement of Investment Disputes (ICSID) tribunal concluded that a port authority, although not a de jure organ of the state, was exercising public powers attributed by law and thus its conduct was imputable to Egypt (ICSID Case No. ARB/04/13, Award, 2008, paras. 156-160). Although the case did not involve cyber activities, its reasoning is instructive. For instance, when a cybersecurity company is tasked by the government to neutralise foreign cyber threats or to administer national-level surveillance programmes, and such delegation is grounded in law or formal mandate, its actions fall within the scope of Article 5. The nature of the power exercised – whether coercive, regulatory or involving sensitive national interests – further reinforces the attribution.

29 "These entities can be, for instance, private or state-owned corporations as well as parastatal entities" (Delerue, 2020, p. 123).

30 Schmitt, 2017, Rule 15, para. 9.

31 H. Tonkin, *State Control over Private Military and Security Companies in Armed Conflict*, Cambridge University Press, 2011, p. 100.

32 The importance of which is confirmed in Jurisdictional Immunities of the State (*Germany v. Italy: Greece intervening*), Judgment, *ICJ Reports 2012*, p. 99, paras. 60-61.

33 Delerue, 2020, pp. 124-125.

34 L. Condorelli, *L'imputation à l'État d'un fait internationalement illicite: solutions classiques et nouvelles tendences*, Brill, 1998, pp. 80-86; Crawford, 2013, p. 137. See, for instance: *Estate of Jean-Baptiste Caire (France) v. United Mexican States* (1929) 5 RIAA 516, 529; *Yeager v. The Islamic Republic of Iran* (1987) 17 Iran-US CTR 92, 110-111; *Petrolane Inc v. The Islamic Republic of Iran* (1991) 27 Iran-US CTR 64, 92.

35 Ibid.; see also ILC, "Draft Articles", 2001, *Commentary to Article 4*, which explains that attribution is based on the capacity in which a person acts, not whether they complied with internal laws or instructions.

36 Schmitt, 2017, Rule 16 and accompanying commentary, which reflects the consensus of international experts that attribution under Article 7 is based on objective institutional and functional criteria.

to the relevant state under international law when the person or entity acts in that capacity, even if it exceeds its authority or contravene instructions.[37]

2.3 Persons or group of persons acting on the instructions of, or under the direction or control of, a state

International law establishes rules to attribute the conduct of private ("non-state") actors to states. Perhaps the most well-known one is the rule by which the conduct of a person or a group of persons is attributed to a state if that person or group of persons acted on the instructions of, or under the direction or control of, that state in carrying out the conduct. This rule is enshrined in Article 8 ARSIWA,[38] and finds support in ICJ case law.[39] It is widely deemed to be applicable with respect to activity in cyberspace,[40] and becomes relevant in order to attribute to states the activity of, inter alia, hackers acting individually or as a group (more or less organised); criminal organisations operating by cyber means; university IT departments; or companies that operate under a state's instructions, direction, or control, but are not empowered by law to exercise elements of governmental authority.[41]

The disjunctive phrasing – instructions, direction or control – is often read as a singular standard of attribution,[42] yet each of them evokes a distinct mode of attribution.[43]

"Instructions" suggests a relatively straightforward exchange between the state and the private actor whereby the state orders, commands or requests a certain conduct by the private entity, which in these cases has been described as acting as an "auxiliary" of the state.[44] This relationship must exist "in respect of each operation in which the alleged violations occurred".[45] The conduct is attributable insofar as it can be traced back to the state's instructions, even if they are not particularly detailed.[46] Therefore, should the private entity act beyond the received instructions, its conduct would not be attributable to the state.[47]

"Direction" is the standard that has received the least scholarly and jurisprudential attention, and is often simply conflated with "control".[48] It has been suggested that "direction" describes a subordination relationship between the state and

---

37 See section 2.1, referring to the rule reflected in Article 7 ARSIWA.

38 ILC, "Articles on Responsibility of States for Internationally Wrongful Acts", GA Res. 56/83, 12 December 2000, art. 8.

39 *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, Merits, *ICJ Reports 1986*, p. 14, paras. 109-115; *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*, Judgment, *ICJ Reports 2007*, p. 43, paras. 398-407.

40 E.g. Council of the European Union, Declaration by the European Union and its Member States on a Common Understanding of the Application of International Law to Cyberspace, (18 December 2024) 15833/24 (EU Common Position), p. 8; Ministry of Foreign Affairs of Japan, Basic Position of the Government of Japan on International Law Applicable to Cyber Operations, 28 May 2021.

41 Schmitt, 2017, pp. 95-96; Mačák, 2016, p. 414.

42 So Crawford, 2013, p. 146. The conflation is noted by Mačák, 2016, p. 411.

43 As implied also by the ILC commentary: ILC, *Report of the International Law Commission on the Work of its Fifty-Third Session* (23 April-1 June and 2 July-10 August 2001), UN Doc A/56/10, 48, Commentary to Article 8, para. 7.

44 Schmitt, 2017, Rule 17, p. 95.

45 *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*, Judgment, *ICJ Reports 2007*, p. 43, para. 400.

46 Mačák, 2016, p. 416; Tsagourias and Farrell, 2020, p. 954.

47 Schmitt, 2017, Rule 17, pp. 97-99, paras. 11-14.

48 Mačák, 2016, p. 411.

the private entity, in which the state "takes the lead"[49] or, more specifically, guides the private entity's conduct short of express instructions.[50] It seems worth highlighting that this implies an ongoing connection between the state and the non-state actor in question: the Stuxnet operation would be an example (should its attribution ever be proved), since it was the result of a long-term project.[51]

By contrast, "control" is the standard that has received the most scholarly and jurisprudential attention, with two competing interpretations put forward respectively by the ICJ and the International Criminal Tribunal for the former Yugoslavia (ICTY).[52]

The majority position in the literature and case law retains *effective control* as the applicable threshold for attribution.[53] The standard requires that the state exercises control over the specific operation giving rise to the wrongful act from its start, through the time it is carried out, to its end, retaining the power to frustrate its success.[54] For instance, one could imagine a case in which a state secretly contracts a software company to embed malicious code into a software program that is widely used in other states, oversees the software's production and ensures the company distributes it to its intended targets.[55] The effective control standard, thus, erects a high threshold, normatively grounded in the aim to avoid the over-extension of state responsibility.[56]

Nonetheless, a minority position, drawing on the ICTY's jurisprudence[57] and supported by some scholars and institutions,[58] has advocated for an *overall control* test as a more suitable standard with respect to organised (armed) groups (while the effective control test would remain the standard for attributing to states the conduct of individuals or (armed) groups that are not sufficiently organised). The "overall control" standard requires that the state both supports and coordinates with the organised non-state armed group – typically by providing financing, training, or resources, and by participating in the organisation or planning of the group's activities.[59]

---

49 Tsagourias and Farrell, 2020, p. 954.

50 Mačák, 2016, p. 418.

51 Ibid., p. 419.

52 See on the point also the relevant sections of the ILC's Commentary to Article 8: ILC, "Draft Articles", 2001, ch. IV, Commentary to Article 8, paras. 4-8.

53 See note 22. With respect to cyberspace, see Government of the Netherlands, "Letter from the Minister of Foreign Affairs to the President of the House of Representatives on the International Legal Order in Cyberspace", 5 July 2019, Appendix: International Law in Cyberspace, p. 6; Brazil, in UNODA (UN Office for Disarmament Affairs), "Official Compendium of Voluntary National Contributions on the Subject of How International Law Applies to the Use of Information and Communications Technologies by States", A/76/136, August 2021, pp. 20-21; Norway, in UNODA, 2021, p. 71; Ireland, "Position Paper on the Application of International Law to Cyberspace", Department of Foreign Affairs, 2023, para. 22, https://www.gov.ie/en/department-of-foreign-affairs/publications/international-law-and-cyberspace/.

54 Mačák, 2016, p. 421; Schmitt, 2017, Rule 17, p. 96, para. 6.

55 The example is provided in ibid., para. 7.

56 Case Concerning the Application of the Convention on the Prevention and Punishment of the Crime of Genocide (*Bosnia and Herzegovina v. Serbia and Montenegro*), Judgment, *ICJ Reports 2007*, p. 43, para. 406; D. Akande, "Classification of Armed Conflicts: Relevant Legal Concepts", in E. Wilmshurst, ed., *International Law and the Classification of Conflicts*, Oxford University Press, 2012, p. 60.

57 *Prosecutor v. Duško Tadić* (Judgment) ICTY-94-1-A (15 July 1999) paras. 115-145. The use of the test as a rule for classifying conflicts under international humanitarian law is less controversial. See *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*, Judgment, *ICJ Reports 2007*, p. 43, para. 404.

58 See e.g., A. Cassese, "The Nicaragua and Tadić Tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia", *European Journal of International Law*, Vol.18, 2007, p. 649; ICRC, "Commentary of 2025 – Convention (IV) Relative to the Protection of Civilian Persons in Time of War", 2025, para. 480, https://ihl-databases.icrc.org/en/ihl-treaties/gciv-1949/Introduction/commentary/2025?activeTab=1949GCs-APs-and-.

59 *Prosecutor v. Duško Tadić* (Judgment) ICTY-94-1-A (15 July 1999) para. 137.

It has been noted that the overall control test may be better suited to attribute conduct in the cyber context, where state involvement is often indirect, anonymised, or routed through proxies whose ties to the state are informal or deniable.[60] Cyber operations may be planned or facilitated by states in ways that intentionally fall below the effective control threshold, allowing them to reap strategic benefits without legal accountability.[61] It is not to be excluded that, by means of general practice and corresponding expressions of *opinio juris*, overall control may emerge as a special rule of attribution for conduct occurring in the cyber context.[62] As a matter of *lex lata*, however, it is premature to conclude that this legal development has already occurred.

Moreover, a test of overall control would not be a panacea to resolve attribution problems that may emerge in the cyber context. The test was developed in the context of armed conflict and applies explicitly to organised armed groups. Many cyber groups – particularly loosely coordinated hacker collectives – may not exhibit the degree of structure or organisation required for the ICTY's threshold to apply.[63] Moreover, even such standard of attribution would fail to capture the full complexity of cyber-related relationships, which may be driven not by hierarchical command, but by ideological convergence, shared strategic aims, or "soft control" mechanisms.[64]

In any case, mere political sympathy or affinity, encouragement, the harbouring of hackers, providing funding or tools, tolerating their activities, or even offering general support are insufficient to establish attribution under Article 8 ARSIWA.

2.4 Other rules for attributing private actors' conduct to a state

Article 9 ARSIWA enshrines the rule by which the conduct of a person or group of persons is attributable to a state: (i) if that person or group of persons is exercising elements of governmental authority; (ii) in the absence or default of the official authorities; and (iii) in circumstances calling for the exercise of such elements of authority. The three cumulative circumstances required by this rule occur extremely rarely in practice, but could in theory also find application in relation to state activity in cyberspace.[65] For instance, one could imagine a scenario – as in the case of internal disturbance or war – in which a state's cyber-related authorities are effectively non-functional and private actors assume control of essential cyber networks or carry out defensive cyber operations in default of official authorities to protect the public interest, stepping in to fulfil roles that normally belong to the government.[66]

Article 10 ARSIWA may also be relevant in the cyber context. This provision allows for the attribution of conduct to a state when it has been carried out by an

60 D. Broeders, E. De Busser and P. Pawlak, "Three Tales of Attribution in Cyberspace: Criminal Law, International Law and Policy Debates", The Hague Program for Cyber Norms Policy Brief, 2020, p. 6; Tsagourias and Farrell, 2020, pp. 961-963.

61 Delerue, 2020, p. 145; Mačák, 2016, pp. 422, 425.

62 Tsagourias and Farrell, 2020, p. 961.

63 Ibid., p. 964.

64 Ibid., pp. 964-965.

65 Delerue, 2020, p. 151; Schmitt, 2017, Rule 15, p. 92, para. 17.

66 For another example, see ibid.

insurrectional movement that later becomes the new government. In the cyber context, it may apply when cyber operations are undertaken by revolutionary groups that subsequently assume state authority.

The rule enshrined in Article 11 ARSIWA attributes conduct to a state "if and to the extent that the State acknowledges and adopts the conduct in question as its own".[67] Pursuant to this rule, specific conduct by a private actor becomes retroactively attributable to a state if that state – at the highest level of government, and in a clear and explicit manner[68] – both identifies the conduct ("acknowledges") and assumes responsibility for it ("adopts"). Mere approval of the conduct or passive benefit derived from it is not sufficient. This rule of attribution could be relevant in the context of state activity in cyberspace.[69] In this regard, it has been suggested that acknowledgement and adoption may occur when a state uses its cyber capabilities to shield an operation by a private actor from measures intended to hinder or stop it, thereby facilitating the operation's continuation.[70]

67 See also *United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran)*, Judgment, *ICJ Reports 1980*, p. 3, paras. 69-74.

68 Tsagourias and Farrell, 2020, p. 955.

69 E.g. Council of the European Union, 2024, p. 8; Ireland, 2023, para. 23.

70 Schmitt, 2017, Rule 17, p. 99, paras. 16-17.

3. Evidentiary issues

Evidence is generally required to substantiate a cyber attribution. It not only confirms whether a cyber incident occurred, but also clarifies critical details such as its timing and the nature, scale, and scope of its (potential) consequences. Furthermore, evidence can help trace the incident's origin, identify the actors behind it, and establish any links between the actors and a state.[71]

However, in practice, collecting and utilising evidence for the purposes of attribution face significant challenges. For instance, it is technically demanding to fully observe and assess the impact of a cyber incident, and tracing the origin of the attack becomes extremely complex when its perpetrators employ advanced obfuscation techniques. Moreover, challenges are exacerbated by the lack of a comprehensive body of rules on evidentiary issues in international law.[72] Questions of evidence and proof – including burden, standard, and methods of proof – were left out of the scope of the ILC work on state responsibility,[73] and are not systematically regulated in the law of international responsibility. Additionally, issues such as whether evidence should be publicly disclosed remain under debate. Therefore, greater attention should be accorded to evidentiary issues.

3.1 Burden of proof

The expression "burden of proof" means that a party seeking to establish a fact – such as the circumstances determining the attribution of an individual's conduct to a state – has to provide the required level of evidence to substantiate its allegation in dispute settlement procedures. With respect to context other than dispute settlement procedures, the Chinese team suggests that the underlying rationale – i.e. the maxim *actori incumbit probatio* – can be more broadly applied even in a bilateral dispute between states,[74] implying that it is generally the victim state that bears the burden of producing the relevant evidence.[75] While recognising that a general expectation of substantiation applies to a state invoking responsibility, the European team nevertheless maintains that the issue of burden of proof – in its technical sense – is more appropriately confined to third-party dispute settlement mechanisms.

In current practice, regardless of whether it is for the purpose of legal attribution, it can also be observed that it is typically the injured state that undertakes the investigation of cyber incidents, collects relevant evidence, and presents it when deemed appropriate, in order to invoke the responsibility of the state to which the conduct in question is attributable.

---

71 M. Roscini, "Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations", in J.D. Ohlin, K. Govern and C. Finkelstein (eds), *Cyber War: Law and Ethics for Virtual Conflicts*, Oxford University Press, 2015, p. 223.

72 Ibid., p.222.

73 ILC, "Articles on State Responsibility", 2000, Commentary to ch. III, para. 4 ("Questions of evidence and proof of such a breach fall entirely outside the scope of the articles"); ibid., Commentary to ch. V, para. 8 ("Just as the articles do not deal with questions of the jurisdiction of courts or tribunals, so they do not deal with issues of evidence or the burden of proof").

74 The Chinese team noted that the ILC did not clearly confine the issue of burden of proof to third-party dispute settlement mechanisms. See ILC, 2000, Commentary to ch. V, para. 8 ("In a bilateral dispute over State responsibility, the onus of establishing responsibility lies in principle on the claimant state").

75 J. Spáčil, "Attribution of Cyber Operations: Technical, Legal and Political Perspectives", *International and Comparative Law Review*, Vol.24(2), 2024, pp. 161-163. H.-G. Dederer and T. Singer, "Adverse Cyber Operations: Causality, Attribution, Evidence, and Due Diligence", *International Law Studies*, Vol.95, 2019, pp. 439-441.

Some have advocated for a reversal of the burden of proof in the cyber context, implying that it falls on the state from whose cyber infrastructure the internationally wrongful act originated to prove that it is not responsible for it.[76] The main argument behind this idea is that in a cyber dispute the state on whose territory or infrastructure the allegedly wrongful conduct occurred would have better access to the knowledge necessary to verify certain facts. However, this research group does not find this reversal to be established in the law as it stands.[77]

3.2 Standard of proof

The expression "standard of proof" refers to the degree of evidence required to substantiate a factual allegation made by a party.[78] Since there is no single standard of proof that would be uniformly applicable before all international dispute settlement mechanisms, the standard required for substantiating a claim must be established on a case-by-case basis.[79] Depending on the varying levels of certainty required, scholars have generally observed the use of four categories of standards of proof: "beyond reasonable doubt", "clear and convincing evidence", "preponderance of evidence" (or preponderance of probabilities, balance of probabilities), and "*prima facie* evidence".[80]

As the highest standard of proof, "beyond reasonable doubt" requires that the evidence presented must be so compelling that it leaves no room for any rational doubt.[81] It is primarily applied in criminal proceedings, reflecting the principle of presumption of innocence,[82] and a similarly stringent standard has been required before the ICJ in cases involving allegations of exceptional gravity.[83]

The "clear and convincing evidence" standard requires the evidence to be highly and substantially more likely to be true than untrue, and the adjudicator must be convinced that the contention is highly probable.[84]

---

76 R.A. Clarke and R.K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, Harper Collins, 2012, p. 249; P. Margulies, "Sovereignty and Cyberattacks: Technology's Challenge to the Law of State Responsibility", *Melbourne Journal of International Law*, Vol.14(155), Winter 2014, p. 296.

77 The Chinese team pointed out that in the 2015 UNGGE report, it was stated that "indication that an ICT activity was launched or otherwise originates from the territory or the ICT infrastructure of a State may be insufficient in itself to attribute the activity to that State" (UNGA, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/70/174, 2015, para. 28(f)). From this, it can be inferred that evidence indicating the activity's source for attribution purposes needs to be provided by the attributing state rather than the territorial state, and based on a standard of proof higher than "*prima facie* evidence". The European team believes that the territorial state maintains a due diligence obligation to, at the very least, stop an ongoing wrongful cyber operation originating from or transiting through its infrastructure.

78 J.A. Green, "Fluctuating Evidentiary Standards for Self-Defence in the International Court of Justice", *International & Comparative Law Quarterly*, Vol.58(163), 2009, p. 58.

79 A. Rajput, "Standard of Proof", *Max Planck Encyclopaedia of International Law*, https://opil.ouplaw.com/display/10.1093/law-mpeipro/e3243.013.3243/law-mpeipro-e3243?rskey=Vri4X5&result=1&prd=MPIL.

80 Roscini, 2015, p. 223; F. Yang, "Pointing with Boneless Finger and Getting Away with It: The Ill-Substantiation Problem in Cyber Public Attribution", in E.Y.J. Lee (ed.), *Revolutionary Approach to International Law: International Law in Asia*, Springer, 2023.

81 "Beyond a reasonable doubt", WEX, https://www.law.cornell.edu/wex/beyond_a_reasonable_doubt; Rajput, "Standard of Proof", para. 55.

82 S. Sayapin, "Presumption of Innocence", *Max Planck Encyclopaedia of International Law*, https://opil.ouplaw.com/display/10.1093/law-mpeipro/e1646.013.1646/law-mpeipro-e1646?d=%2F10.1093%2Flaw-mpeipro%2Fe1646.013.1646%2Flaw-mpeipro-e1646&p=emailA8QRz%2FhKrKYXw.

83 Even though the ICJ did not use the expression "beyond reasonable doubt", its requirement of "fully conclusive" evidence for allegations of particular gravity reflects a very high standard of proof, approaching that level: see Case Concerning the Application of the Convention on the Prevention and Punishment of the Crime of Genocide (*Bosnia and Herzegovina v. Serbia and Montenegro*), Judgment, *ICJ Reports 2007*, p. 43, paras. 209 and 422.

84 S. Wilkinson, *Standards of Proof in International Humanitarian and Human Rights Fact-Finding and Inquiry Missions*, Geneva Academy of International Humanitarian Law and Human Rights, n.d., p. 17; Rajput, "Standard of Proof".

The "preponderance of evidence" standard refers to evidence that carries more weight and is more persuasive than the opposing evidence.[85]

The term "*prima facie* evidence" denotes evidence that, while only indicative, is sufficient to substantiate a fact or give rise to a presumption of its truth, unless it is successfully rebutted.[86]

Establishing a uniform standard of proof for attribution related to cyber operations is impractical. The prevailing view holds that a sliding scale theory could be adopted,[87] meaning that the level of proof required should depend on the severity of the response that the state intends to implement in response to an internationally wrongful act.[88]

The European team notes that outside of adjudicative mechanisms, international law does not prescribe a specific evidentiary standard for attribution. In contexts such as countermeasures, retorsion, or self-defence, states act unilaterally, and the legal risk lies in the possibility that erroneous attribution may itself give rise to an internationally wrongful act.[89]

The Chinese team, however, contends that, in terms of responses such as countermeasures and self-defence, states can act unilaterally, but they should do so based on an evidentiary standard that meets a certain threshold,[90] although uncertainty remains as to whether this threshold can be clearly defined. In this respect, it can been noted that certain states have highlighted in their position papers from the legal perspective the necessity of attaining "a sufficient degree of certainty"[91] and "a sufficient level of confidence".[92] However, these formulations still fall short of specificity, but the basic consideration is nonetheless relatively clear, i.e. the standard should neither be set unreasonably high, just as Estonia advocates for a reasonable, rather than absolute, level of certainty,[93] nor be unduly lowered, as Brazil argues, but difficulties must not serve as a justification to lower the bar for determinations on attribution.[94] Therefore, it remains to be seen how national practices will develop concerning the standard of proof for cyber attribution.

---

85 T. Renno, "Preponderance of Evidence", *Max Planck Encyclopaedia of International Law*, https://opil.ouplaw.com/display/10.1093/law-mpeipro/e2782.013.2782/law-mpeipro-e2782.

86 "Prima Facie", *Black's Law Dictionary*, https://thelawdictionary.org/prima-facie/.

87 Green, 2009, p. 58; Dederer and Singer, 2019, pp. 444-445; for a national position, see Government of the Netherlands, Appendix: International law in cyberspace, September 2019, p.7.

88 This observation falls in line with the *Tallinn Manual*'s suggestion that "the greater the underlying breach … the greater the confidence ought to be in the evidence relied upon by a State considering a response" (Schmitt, 2017, p. 82). See also Oil Platforms (*Islamic Republic of Iran v. United States of America*), Separate Opinion of Judge Higgins, *ICJ Reports 2003*, p. 225, para. 33; and T. Mikanagi and K. Mačák, "Attribution of Cyber Operations: An International Law Perspective on the Park Jin Hyok Case", *Cambridge International Law Journal*, Vol.9, pp. 51, 66.

89 ILC, "Draft Articles", 2001, ch. II, Commentary to Article 49, para. 3.

90 J. K. Davis, "Developing Applicable Standards of Proof for Peacetime Cyber Attribution", Tallinn Paper no. 13, 2022.

91 Czech Republic, Position paper on the application of international law in cyberspace, February 2024, p. 14, para 57, available at https://nukib.gov.cz/en/infoservis-en/news/2093-the-czech-republic-has-published-a-position-paper-on-the-application-of-international-law-in-cyberspace/ (visited 25 November 2025).

92 Germany, On the Application of International Law in Cyberspace – Position Paper, March 2021, p. 11, available at https://www.auswaertiges-amt.de/blob/2446304/2ae17233b62966a4b7f16d50ca3c6802/on-the-application-of-international-law-in-cyberspace-data.pdf (visited 25 November 2025).

93 UNGA, Official Compendium of Voluntary National Contributions on the Subject of How International Law Applies to the Use of Information and Communications Technologies by States, A/76/136, 13 July 2021, Estonia, p. 28.

94 UNGA, Official Compendium of Voluntary National Contributions on the Subject of How International Law Applies to the Use of Information and Communications Technologies by States, A/76/136, 13 July 2021, Brazil, p. 21.

3.3 Method of proof

Various methods exist for proving the authorship and modalities of cyber operations, as well as the existence of the requisite relationship for attribution (such as instructions, directions or control). Such methods encompass documentary evidence, official statements, inquiries and expert testimony. Given the technical nature of cyberspace, digital evidence collected through digital forensics often plays a particularly important role.

Therefore, digital forensic evidence, together with other intelligence available after any cyber operation, may at times only support inferences that cumulatively lead to a conclusion.[95] As in other domains, the probative value of such evidence depends not on its digital character, but on the inferential steps it supports in establishing attribution. Thus, the cyber domain has not fundamentally transformed the available methods of proof that can be employed. This includes AI-assisted analytical tools, which may help to process large volumes of data, but do not themselves alter the applicable evidentiary standards or the need to justify the inferential steps underlying attribution. At the same time, while using AI-assisted tools can markedly enhance the capacity to process and correlate large volumes of data, their use may also introduce additional legal and methodological considerations, particularly with respect to the transparency of the analytical process and the explainability and verifiability of the resulting outputs. As such, the admissibility and probative value of AI-generated analyses may warrant closer examination.

3.4 Admissibility of proof

An important issue arises as to whether evidence collected in a manner that violates international law can be deemed admissible, should the relevant dispute proceed to dispute settlement mechanisms. As mentioned above, there may be a strong need in the cyber context to conduct digital forensic activities in the territory of the target state. However, these forensic activities are often carried out covertly, without the authorisation of the target state, and there is a potential risk of infringing rules of international law protecting that state's sovereignty. Nevertheless, such evidence may still be admitted, albeit this would not exclude the illegality of the method of collection, and its admissibility would ultimately depend on the forum concerned.[96]

Outside the dispute settlement mechanisms, since there is no supranational body to determine the admissibility of evidence, the decision on whether to rely on such evidence rests with the unilateral decision of the state concerned. In practice, it may happen that evidence obtained through unlawful means is used for cyber-related attribution purposes.

---

95 S. Aravindakshan, "Cyberattacks: A Look at Evidentiary Thresholds in International Law", *Indian Journal of International Law*, Vol.59, 2021, p. 292.

96 Corfu Channel (*U.K. v. Alb.*), Judgment, 1949 ICJ 4, 14-15, cited in Roscini, 2015, pp. 246-247. See also S. Mansour Fallah, "Illegally Obtained Evidence: International Adjudication", in *Max Planck Encyclopedia of Public International Law*, paras. 6-8, 31, noting that the ICJ and other inter-state courts have no explicit rules on illegally obtained evidence and that no generally binding rule of inadmissibility has emerged; the ICJ in *Corfu Channel* condemned the unlawful method of evidence gathering, but nevertheless relied on the resulting material.

However, the Chinese team notes that, in the absence of explicit authorisation under treaty law or customary international law, the admissibility of such evidence should be evaluated by reference to general principles of law. In particular, under the principle of good faith, evidence procured through illegal means should, in principle, not be accepted.[97] In other words, unlawfully obtained evidence should not serve as the basis for public attribution. At the same time, general principles such as the clean hands doctrine and the prohibition of unjust enrichment further suggest that unilateral responses taken on the basis of such attribution should not be regarded as lawful.

The European team, while recognising the need to respect international law in the collection of evidence, notes that the unlawfulness of the method of collection does not preclude per se a state from relying on such evidence for purposes of attribution outside of dispute settlement processes. In this view, the lawfulness of the subsequent reliance on evidence is distinct from that of its acquisition, although the latter may give rise to separate responsibility. As such, the unlawfulness inherent in the collection process does not in and of itself invalidate the attribution or render a unilateral response (such as a countermeasure) unlawful, provided that the attribution itself is correct. However, under such circumstances, the state must also bear the responsibility for the unlawfulness of the evidence collection activity itself.

3.5 Evidentiary issues in public attribution

Currently, an increasing number of countries are engaging in public cyber-related attribution. To make their allegations more persuasive, at times states may appear to implicitly refer to evidentiary standards. Officials often use terminology such as "highly likely", "almost certain", "we have evidence that ...", etc. to signal the strength of the evidence supporting attribution. The stronger the evidence on which attribution is based, the stronger is the allegation's credibility and potential to secure political and diplomatic support, in line with the 2015 UNGGE report's suggestion that "the accusations of organizing and implementing wrongful acts brought against States should be substantiated".[98]

Among the countries that have stated their national positions on how international law applies in cyberspace, none has expressed that evidence on which public attribution is based must be disclosed as a matter of law.[99] Of course, a state may still decide to disclose evidence based on political or other considerations. As stated by Germany, clarifying the allegations that have been raised can enhance the transparency, legitimacy, and general acceptance of decisions on attribution and any response measures taken.[100]

---

97 Ibid, para.44.

98 UNGA, 2015, para. 28(f).

99 Of note, Russia has pointed out that "one should refrain from publicly imposing responsibility for an incident in information space on a particular State without supplying necessary technical evidence" (UNGA, Official Compendium of Voluntary National Contributions on the Subject of How International Law Applies to the Use of Information and Communications Technologies by States, A/76/136, 13 July 2021, Russian Federation, p. 80).

100 Federal Republic of Germany, "On the Application of International Law in Cyberspace", Position Paper, Federal Foreign Office, March 2021, p. 12.

The Chinese team notes that making a public attribution without disclosing the supporting evidence inevitably increases the risk of false or erroneous attributions and, even more seriously, may trigger unjustified self-defence or countermeasures against the state that is alleged to be responsible for the relevant internationally wrongful act.[101] Responses based on false or erroneous attribution may incur international responsibility of their own. However, false or erroneous attributions not followed by acts of self-defence or countermeasures, while having the potential to result in reputational damage that could erode the attributing state's credibility and influence future diplomatic or multilateral discussions, may not amount to an internationally wrongful act per se.[102] The Chinese team believes that further study on this matter would be warranted.

101 F. Yang, "The Problem With Ill-Substantiated Public Cyber Attribution: A Legal Perspective", in A.E. Levite et al. (eds), *Managing U.S.-China Tensions Over Public Cyber Attribution*, Carnegie Endowment for International Peace and Shanghai Institutes for International Studies, 2022, p. 12.

102 Ibid.

Building Peace Together

GCSP
Geneva Centre for Security Policy

Geneva Centre for Security Policy
Maison de la paix
Chemin Eugène-Rigot 2D
P.O. Box 1295
1211 Geneva 1
Switzerland
Tel: + 41 22 730 96 00
Contact: www.gcsp.ch/contact
www.gcsp.ch

ISBN: 978-2-88947-034-1