The Problem of Cyber Attribution Between States

https://www.e-ir.info/2020/05/06/the-problem-of-cyber-attribution-between-states/

CLARA ASSUMPçãO, MAY 6 2020

Attributing responsibility to who perpetrated an attack against a state and, even more importantly, who ordered it, is a way to achieve cyber deterrence. However, cyber attribution, particularly between states, is a thorny affair. International Law establishes that states should warn other states before attacking, and that states are responsible for the actions of non-state actors under their control.[1] These rulings are translated to the cybersphere, albeit not respected.[2] Accomplishing a perfect attribution in a context of diffuse actors and false flag operations is also beyond the technical and strategic capabilities of most states. In this context, establishing a legal baseline over which to build regulations is an important step.

In this paper, I aim to answer how sure a state should be to attribute a cyberattack, and what should be the threshold for attribution. To do so, I will first discuss in deeper detail what cyber attribution is, its layers and graduations. Then, I will flesh out how attribution poses a problem to states in terms of feasibility, quality and usefulness. In the third section of this paper, I will elaborate on how international law approaches the subject of attribution and will explain, compare and critically analyse the different doctrines on state control over non-state actors. Finally, I will conclude that public international attribution is more than a technical issue, but a strategic and political affair. Thus, a state should weigh the political stakes of making such call regardless of its certainty regarding the quality of its attribution. I will also defend that, due to the difference in the circumstances of the states dealing with cyberattacks, there should be no fixed doctrine on state control, but each case should be ruled ad hoc.

What is cyber attribution and why does it pose a problem to states?

Traditionally, cyber attribution refers to allocating the responsibility of an attack to an attacker or group of attackers, and subsequently, unveiling their real-world identity.[3] However, when discussing cyber attribution between states, unveiling the identity of the attacker is not enough. International cyber attribution is a complex process that puts together and tests two different layers of investigation: technical and strategic. The technical attribution deals with the direct proofs of the cyberattack, meaning the digital forensic evidence. It studies the computer code and modularity of the software used in the assault, the network activity during the event, and the language artefacts of the software and the system behind it, for example. Technicians will also investigate the type of targeting, which vulnerabilities the malicious software exploited, how it entered the victim's system and what the intruder was looking for.[4] Due to false flag operations and spoofing techniques, the chances of achieving perfect technical attribution are low.[5]

The more elaborate the attack, the harder it is to attribute. Even perfect technical attribution, however, will only go as far as identifying the individual or group behind the attack. Nevertheless, in cyber attribution between states, the core question is not "Who did it?", but "Who is to blame?"[6] In order to define the responsibility for the attack, a strategic layer of investigation is also necessary. This will analyse the human aspects of the operation, such as the patterns of life of the attack[7] and the level of resources invested in it. This analysis, joined with a study of the geopolitical context, history, politics and information gathered through intelligence, helps shed light on the attacker's potential influence or backing from hostile states.[8] Cyber attribution is thus a political judgment based on technical and strategic information. As such, it is not a binary or absolute affair, but one that is gradual and may oscillate from low to high-quality. States ponder over the political stakes when making a public attribution. [9] Regardless of how sure they are over the quality of their claim, public international attributions are political actions and a state's prerogative.

Attribution poses a problem not only with regard to its feasibility and quality but also regarding its usefulness. The main goal of publicising a cyber attribution is deterrence – the victim is making it known that it has enough capabilities to identify the perpetrators, and as such, emphasise its ability to punish and retaliate. However, in the case of states, deterrence is not always achieved. Boebert comes forth with scenarios that help elucidate this dilemma. He highlights four potential cases of cyberattacks on states: 1. Attacks that are directly planned and organised by a state without the use of non-state actors; 2. Attacks that are planned and sponsored by a state, but executed through non-state actors; 3. Attacks that are tolerated by the host country and executed by non-state actors; and 4. Attacks that are planned and executed by non-state actors with no involvement of any state.[10]

In the first case, public attribution would have little effect in terms of deterrence, as it would most probably take place in an environment of international tension and imminent direct conflict. Public attribution, in this instance, could even be the trigger for war. In the second case, the involvement of non-state actors brings a cloak of plausible deniability to the state, making attribution obscured. The individual or group behind the attack would also be under the protection of the organising state, making it harder to enforce prosecution. In the third case, attribution is even more obscure, as there are no overt detectable links between the attackers and the organising state. The individual or group behind the attacks might be vulnerable to prosecution, but deterrence from attacks backed by states is not achieved. Finally, the fourth scenario is the only where deterrence is achieved through public cyber attribution. The organiser of the attack, being a non-state actor, is uncovered and at the mercy of a much more powerful actor, making the promise of harsh punishment enough to act as deterrence from similar attacks.[11]

Thus, cyber attribution is an intricate process that does not work in binaries, but rather in a scale of quality where absolute certainty is impossible. Making attribution public aims to increase cyber deterrence. However, this tactic may not work for states dealing with direct or indirect attacks by another state. The complexity of this situation is increased by the lack of a clear standard in international law on how to deal with state responsibility in cyberattacks. In the next section, I will briefly analyse the two main legal regimes used in such cases: the Effective Control Doctrine and the Overall Control Doctrine.

Two approaches to solving the attribution problem

In International Law, states are required to identify themselves when attacking another state. This interpretation is extended beyond conventional means of attack and also encompass the cyberspace.[12] As stated in The Hague Convention:

The contracting Powers recognise that hostilities between themselves must not commence without previous and explicit warning, in the form either of a declaration of war, giving reasons, or of an ultimatum with conditional declaration of war.[13]

The Article VIII of the International Law Commission's Draft on the Responsibility of States for International Wrongful Acts also states, in an interpretation also expandable to the cybersphere,[14] that:

The conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct.[15]

Additionally, the Tallinn Manual 2.0 specifically approaches the issue of attribution and responsibility in cyberattacks with the following rulings:

Rule 14 – Internationally wrongful cyber acts. A State bears international responsibility for a cyber-related act that is attributable to the State and that constitutes a breach of an international legal obligation.[16]

Rule 15 – Attribution of cyber operations by State organs. Cyber operations conducted by organs of a State, or by persons or entities empowered by domestic law to exercise elements of governmental authority, are attributable to the State.[17]

Rule 17 – Attribution of cyber operations by non-State actors. Cyber operations conducted by a non-State actor are attributable to a State when:

(a) engaged in pursuant to its instructions or under its direction or control; or

(b) the State acknowledges and adopts the operations as its own.[18]

Thus, it is widely understood and agreed upon that states should not attack other states without identifying themselves; and that states bear responsibility for attacks by non-state actors that are under their control. There is, however, controversy on how to interpret 'state control.' The two most widely used interpretations are the Effective Control Doctrine and the Overall Control Doctrine.

The Effective Control Doctrine (ECD) originated in the International Court of Justice Nicaragua case and recognises state control over non-state actors only when those actors perform in complete dependence on the state. The standard for this doctrine is that effective control be proven beyond any doubt.[19] The burden of the proof is almost impossible to satisfy,[20] and the odds are even lower for states that do not have the financial and/or technical resources to safeguard their cyberspace to Western standards. However, Effective Control Doctrine also protects those same states from accusations of complicity in attacks originating from their territory, and allows them not to relinquish sovereignty over their cyberspheres.

ECD was the legal regime applied to Russia in the case of the cyberattacks on Georgia during the Russo-Georgian War of 2008. There is no proof beyond any doubt that Russia was behind the operation,[21] however, the coordination of the attacks with the events in the battlefield along with forensic evidence provide a strong indication that the Kremlin was facilitating the manoeuvre. Russia, however, stated that the attackers were Russian patriots and the government had absolutely no influence over them.[22] This case highlights the main downside of ECD – that is, how the requirement of proof beyond any doubt clashes with the actual impossibility of providing perfect technical and strategic confirmation of the authorship of a cyberattack when non-state actors and plausible deniability are involved. This incompatibility leads to claims that the "attribution fixation" of the ECD is a de facto license for impunity in the cybersphere.[23]

The Overall Control Doctrine (OCD), on the other hand, originated in the International Criminal Tribunal for the Former Yugoslavia Tadic case, and it holds that a state is responsible for the actions of non-state actors whenever it has a role in organising, coordinating or providing support for the group. In the OCD, the standard is that overall control be proven beyond a reasonable doubt.[24] This standard is more compatible with the current technical and strategic limitations of cyber attribution. Applied to the Russo-Georgian case, Russia would have been considered accountable for the cyberattacks on Georgia, as forensic and strategic evidence point to Kremlin's influence and coordination over the 'cyber-patriots.'

Amongst those favourable to mainstreaming the OCD, there are some who campaign for transforming cyber attribution into cyber responsibility. In this framework, states would be responsible for attacks originating from their territory or steered by their citizens, regardless of existing any state control over the perpetrators or not. Ignoring, abetting or conducting an attack would incur in responsibility, whereas states that are effective in protecting their cyberspace and prohibiting cyberattacks would be exempt.[25] This view, however, is not feasible beyond the Western sphere, as not many developing countries would have the capacity or willingness, in a context of limited resources, to focus investment in cybersecurity when it does not even affect their own state directly. In a context of mainstreamed cyber responsibility, a likely scenario would be that third-world countries, afraid of being made accountable for attacks they have no means to control, would relinquish the supervision of their cyberspace to developed countries, in a gesture that could be potentially harmful to their sovereignty and security, and akin to cyber-imperialism.

Whereas the Effective Control Doctrine establishes a too-high of a threshold for attribution, requiring proof beyond any doubt; the Overall Control Doctrine might become too lenient in its demands of proof beyond a reasonable doubt, transferring the discussion from what 'state control' is to what 'reasonable doubt' might be. Thus, there should not be

a fixed threshold for attribution, and the doctrine applicable to each case is best decided ad hoc. This comes at a loss of a baseline for regulatory responses but establishes a legal system that is more capable and fair in its rulings over states that vary widely in control capacity and resources.

Conclusion

Cyber attribution between states is a complex affair that involves a layer of technical and strategic investigation. The more elaborate the attack, the harder it is to attribute, making for the chances of achieving perfect attribution very low. The odds are even lower in the case of attacks engendered by hostile states but executed by non-state actors. Cyber attribution, thus, is not a binary of proving guilty or not guilty with absolute certainty. Publicising a cyber attribution is, thus, a pragmatic judgment prerogative of the state and that will be based on technical and strategic information, as well as on analysis of the political stakes.

Another problem posed by attribution is the extent to which states should be responsible for the actions of non-state actors under its cyber-jurisdiction. The Effective Control Doctrine dictates this responsibility can only be attributed if effective control between the state and the non-state actor involved in the attack is proven beyond any doubt. The Overall Control Doctrine, on the other hand, rules that if the state can be proven, beyond a reasonable doubt, to be involved organising, coordinating or supporting the cyberattack engendered by the non-state actor, the responsibility should then fall to the state.

Requiring proof beyond any doubt is not compatible with the limitations in attribution. Although it is important to have a baseline for regulatory responses, it is more important to guarantee a fair legal system. In this trade-off, the best solution is to keep the definition of state control ad hoc, ensuring rulings that, even if sometimes lenient, are flexible to deal with the wide diversity that exists between states when it comes to capabilities and resources available to cybersecurity.

Thus, the attribution problem should not be solved, but managed.[26] The certainty to which states must adhere to in order to attribute a cyberattack is not fixable and depends on political calculations as well as on the seriousness of the incident. The threshold for attribution should also not be stagnant, as holding every state to the same standard of what state control is might lead to solutions that violate autonomy and sovereignty, hindering development. The cyberspace is dynamic, flexible and widely adaptable. In order to regulate cybercrimes, states and international law should strive to be the same way.

Notes:

[1] Second International Peace Conference, Hague Convention (III) on the Opening of Hostilites, 1910; Fifth-third session of the International Law Comission, ‘Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries – 2001’.

[2] Boebert, ‘A Survey of Challenges in Attribution’, 201.

[3] Saalbach, ‘Attribution of Cyber Attacks’.

[4] Rid and Buchanan, ‘Attributing Cyber Attacks’, 12–17.

[5] Boebert, ‘A Survey of Challenges in Attribution’, 50.

[6] Healey, ‘Beyond Attribution’, 1.

[7] For example, if they coincide with the working hours of a governmental institution, as was the case of the PLA attacks on the United States from 2006 to 2014.The United States Department of Justice, ‘U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage’; Rid and Buchanan, ‘Attributing Cyber Attacks’, 19.

[8] Rid and Buchanan, 'Attributing Cyber Attacks', 13–19.

[9] Rid and Buchanan, 7, 30.

[10] Boebert, 'A Survey of Challenges in Attribution', 50–51.

[11] Boebert, 50–51.

[12] Shackelford, 'State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem', 201.

[13] Second International Peace Conference, Hague Convention (III) on the Opening of Hostilites, 1910.

[14] Shackelford, 'State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem', 201.

[15] Fifth-third session of the International Law Comission, 'Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries – 2001'.

[16] Schmitt, 'Law of International Responsibility', 84.

[17] Schmitt, 87.

[18] Schmitt, 94.

[19] Shackelford, 'State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem', 198–201.

[20] Shackelford, 203.

[21] Schapp (2009) cited in Shackelford, 205.

[22] Connell and Vogler, 'Russia's Approach to Cyber Warfare', 17.

[23] Healey, 'Beyond Attribution'.

[24] Shackelford, 'State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem', 198–201.

[25] Healey, 'Beyond Attribution', 1–3.

[26] Rid and Buchanan, 'Attributing Cyber Attacks', 31.

Bibliography

Boebert, W. Earl. 'A Survey of Challenges in Attribution'. In*Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*. Washington, D.C.: National Academies Press, 2010. https://doi.org/10.17226/12997.

Connell, Michael, and Sarah Vogler. 'Russia's Approach to Cyber Warfare'. CNA Analysis & Solutions. Arlington County, Virginia: The CNA Corporation, March 2017. https://www.cna.org/cna_files/pdf/DOP-2016-U-014231-1Rev.pdf.

Fifth-third session of the International Law Commission. 'Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries – 2001'. *State Responsibility*, 2001, 114.

Healey, Jason. 'Beyond Attribution: Seeking National Responsibility for Cyber Attacks'. Issue Brief. Washington,

D.C.: Atlantic Council, 22 February 2012. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/beyond-attribution-seeking-national-responsibility-in-cyberspace/.

Rid, Thomas, and Ben Buchanan. 'Attributing Cyber Attacks'. *Journal of Strategic Studies* 38, no. 1–2 (2 January 2015): 4–37. https://doi.org/10.1080/01402390.2014.977382.

Saalbach, Klaus-Peter. 'Attribution of Cyber Attacks'. In *Information Technology for Peace and Security: IT Applications and Infrastructures in Conflicts, Crises, War, and Peace*, edited by Christian Reuter, 279–303. Wiesbaden: Springer Fachmedien, 2019. https://doi.org/10.1007/978-3-658-25652-4_13.

Schmitt, Michael N., ed. 'Law of International Responsibility'. In *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed., 79–167. Cambridge: Cambridge University Press, 2017. https://doi.org/10.1017/9781316822524.010.

Second International Peace Conference, The Hague. Hague Convention (III) on the Opening of Hostilites, 1910, Pub. L. No. Art. 1 (1907). https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Article.xsp?action=openDocument&documentId=7970026C4242952EC12563CD005164BB.

Shackelford, Scott J. 'State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem', n.d., 12.

The United States Department of Justice. 'U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage'. Justice News, 19 May 2014. https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

Written by: Clara Assumpção
Written at: Charles University
Written for: Lucie Kadlecová, M.A.
Date written: 01/2020