Shared Responsibility for Cyber Operations

Boutin, B.

DOI
10.1017/aju.2019.31
Publication date
2019
Document Version
Final published version
Published in
AJIL unbound

doi:10.1017/aju.2019.31

SYMPOSIUM ON CYBER ATTRIBUTION

SHARED RESPONSIBILITY FOR CYBER OPERATIONS

*Berenice Boutin**

When the responsibility of more than one state is engaged in relation to a wrongful cyber operation, the relevant states share responsibility for it. Shared responsibility can arise, for instance, when multiple states jointly conduct a cyber operation or when one state is involved in the cyber operation of another state (e.g., by providing assistance or exercising control). In view of the persistent difficulties associated with attribution of cyber conduct, shared responsibility can be a useful analytical framework to broaden the net of possible responsible states in relation to a cyber operation.

As this symposium explores, it is often difficult to identify the author(s) of a cyber operation. Difficulties arise in locating the origin of an attack or identifying its perpetrator(s). Attribution of conduct is further complicated because many types of infrastructure can be hacked and operations that appear to be conducted by one state might be covertly directed by another.[1] This essay explores opportunities to seek the responsibility of all states that directly or indirectly contribute to a cyber operation.

The Notion of Shared Responsibility for Cyber Operations

Shared responsibility is a relatively less developed area of the law of state responsibility, and the International Law Commission (ILC) Draft Articles on the Responsibility of States for Internationally Wrongful Acts (ARSIWA) and their commentaries[2] offer limited guidance on the determination and consequences of responsibility in situations where the conduct of multiple states combines to cause an injury. Recent practice in other fields of international law illustrates how the responsibility of coperpetrators or complicit states can be engaged, so as to reach states that are not necessarily the main perpetrator of a wrongful conduct. For instance, the European Court of Human Rights affirmed the responsibility of certain European states that assisted U.S.

* *Researcher at the Asser Institute (The Hague), and member of the SHARES Project on Shared Responsibility in International Law (University of Amsterdam). The views expressed in this essay are those of the author and do not necessarily reflect the views of the SHARES Project as such.*

[1] Constantine Antonopoulos, *State Responsibility in Cyberspace*, *in* Research Handbook on International Law and Cyberspace, (Nicholas Tsagourias & Russell Buchan eds., 2015); William Banks, *State Responsibility and Attribution of Cyber Intrusions after* Tallinn 2.0, 95 Tex. L. Rev. 1487 (2017); Peter Margulies, *Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility*, 14 Melb. J. Int'l L. 496 (2013); Michael N. Schmitt & Liis Vihul, *Proxy Wars in Cyberspace: The Evolving International Law of Attribution*, 1 Flet. Sec. Rev. 55 (2014).

[2] UN Int'l Law Comm'n, Draft Articles on the Responsibility of States for Internationally Wrongful Acts (2001), Report of the ILC on the Work of its Fifty-Third Session, UN GAOR 56th Session Suppl. No. 10, A/56/10, at. 26–30 [hereinafter ARSIWA]; UN Int'l Law Comm'n, Draft Articles on the Responsibility of States for Internationally Wrongful Acts, with commentaries (2001), Report of the ILC on the Work of its Fifty-Third Session, UN GAOR 56th Session Suppl. No. 10, A/56/10, at 30–143 [hereinafter ARSIWA Commentaries].

rendition operations.[3] In the context of peacekeeping operations, domestic courts have occasionally upheld the responsibility of troop-contributing states for conduct for which the United Nations allegedly shared responsibility but could not be brought to court in view of its immunity.[4] The SHARES Project on Shared Responsibility in International Law, carried out at the University of Amsterdam, extensively researched the foundations and implications of shared responsibility,[5] and this essay draws on some of the project's findings.

Next to attribution of conduct, the second requirement to hold a state internationally responsible is that the operation must be in violation of an international norm binding on that state.[6] For instance, cyber intrusions involving sabotage or destruction of a state's critical infrastructure can amount to breach of the prohibition to use of force.[7] Other forms of cyber interference can qualify as a breach of the principle of nonintervention.[8] In the context of mass surveillance and data interception, human rights obligations with regard to privacy might be relevant.[9] This essay does not address whether a certain cyber operation qualifies as a breach of international law and therefore possibly engages responsibility. Rather, it proceeds on the assumption that a given operation breached an applicable norm and focuses on the determination and consequences of responsibility for cyber operations in situations where multiple states are allegedly involved.

The following sections explore three of the scenarios of shared responsibility most relevant in the context of cyber operations: joint conduct, aid or assistance, and lack of due diligence. Each section addresses the conditions in which shared responsibility for cyber operations can arise and the consequences entailed by shared responsibility in terms notably of reparation.

Multiple Attribution of a Joint Cyber Operation

Shared responsibility can arise when the same wrongful cyber operation is attributed to more than one state. The ILC noted in the ARSIWA Commentaries that, by application of Articles 4–11 ARSIWA, "the same conduct may be attributable to several States at the same time."[10] For instance, the conduct of a common organ or entity established by several states and acting on their behalf is attributed to each of these states.[11] Multiple attribution of conduct can also arise with respect to joint conduct, where two or more states "combine in carrying out together an internationally wrongful act in circumstances where they may be regarded as acting jointly in respect of the

[3] El-Masri v. the Former Yugoslav Republic of Maced., App. No. 39630/09, Eur. Ct. H.R. (2012) [hereinafter El-Masri]; Abu Zubaydah v. Lith., App. No. 46454/11, Eur. Ct. H.R. (2018).

[4] HR 06 september 2013, Zaaknummer 12/03324 (Neth./Nuhanović) (Neth.); HR 13 april 2012, Zaaknummer 10/04437 (Stichting Mothers of Srebrenica/Neth.) (Neth.).

[5] Principles of Shared Responsibility in International Law: An Appraisal of the State of the Art (André Nollkaemper & Ilias Plakokefalos eds., 2014); Distribution of Responsibilities in International Law (André Nollkaemper & Dov Jacobs eds., 2015); The Practice of Shared Responsibility in International Law (André Nollkaemper & Ilias Plakokefalos eds., 2017); *See also* SHARES Project.

[6] ARSIWA, *supra* note 2, art. 2.

[7] Marco Roscini, *Cyber Operations as a Use of Force*, *in* Research Handbook on International Law and Cyberspace (Nicholas Tsagourias & Russell Buchan eds., 2015).

[8] Sean Watts, *Low-Intensity Cyber Operations and the Principle of Non-Intervention*, *in* Cyber War: Law and Ethics for Virtual Conflicts (Jens David Ohlin et al. eds., 2015).

[9] Schmitt & Vihul, *supra* note 1, at 61.

[10] ARSIWA Commentaries, *supra* note 2, at 33–34 (commentary to art. 1(6)).

[11] *Id.* at 44 (commentary to art. 6(3)); Certain Phosphate Lands in Nauru, (Nauru v. Austl.), Preliminary Objections, 1992 ICJ Reports 240, paras. 45–47 (June 26).

entire operation."[12] A joint act is attributed to each state that, acting through its own organs, coauthored the wrongful act.[13]

In view of the covert nature of many cyber operations, it is unlikely that states would set up a common organ to deploy operations. The scenario of joint conduct could, however, be relevant. For instance, the Stuxnet malware deployed as part of Operation Olympic Games was reportedly developed together by American and Israeli secret agencies in "unusually tight collaboration."[14] According to the *New York Times*, the United States initiated the project of targeting Iranian nuclear facilities in Natanz, and Israel soon became an equal partner in developing and launching the operation. Israel "had technical expertise that rivaled" that of the United States and "deep intelligence about operations at Natanz that would be vital to making the cyberattack a success."[15] In these circumstances, it can be argued that Stuxnet was a joint cyber operation attributable to both the United States and Israel.

In situations of multiple attribution, injured parties are entitled to invoke the responsibility of each responsible state for the whole cyber operation, and can seek full reparation from each of the coresponsible states. Indeed, "responsibility is not diminished or reduced by the fact that one or more other States are also responsible for the same act."[16] In other words, states that jointly engage in a wrongful cyber operation bear joint and several liability for it.[17]

Aid or Assistance to the Cyber Operation of Another State

A second scenario is that of state responsibility for aid or assistance, which arises when one state aids or assists another state in conducting a cyber operation. Under this form of derived responsibility (also referred to as "responsibility in connection with the act of another State"),[18] the assisting state is not responsible for the cyber operation as such but for the support that it provided to the operation. The question is not whether the main wrongful conduct can be attributed to several states but whether states other than the main perpetrator bear responsibility for their own conduct that contributed to or facilitated the cyber operation of another state.

Aid or assistance can take diverse forms, including tangible and noncyber forms of support that do not pose the same attribution hurdles as cyber conduct. Therefore, while the conduct of the assisting state still needs to be attributed, the element of attribution might be easier to demonstrate. Examples of aid or assistance to the cyber operation of another state could include providing technical assistance to another state, sharing (part of) malware code or other tools and techniques, gathering and sharing specific intelligence or other necessary data, or lending strategic facilities.

The conditions for responsibility for aid or assistance to another state are found in Article 16 ARSIWA, which tentatively codifies customary international law. It provides that a state is responsible for aid or assistance when it knowingly facilitates the wrongful conduct of another state. In the ILC Articles, the standard is one of actual knowledge, whereby it must be shown that the assisting state knew that its support would be used to commit a

[12] ARSIWA Commentaries, *supra* note 2, at 124 (commentary to art. 47(2)).

[13] *Id.*; UN Int'l Law Comm'n, Report on the Work of Its Thirtieth Session (1978), UN GAOR 33rd Session, Suppl. no. 10, at 99.

[14] David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, N.Y. Times (June 1, 2012). *See also* Nate Anderson, *Confirmed: US and Israel Created Stuxnet, Lost Control of It*, Ars Technica (June 1, 2012).

[15] Sanger, *supra* note 14.

[16] ARSIWA Commentaries, *supra* note 2, at 124 (commentary to art. 47(1)).

[17] James Crawford (Special Rapporteur on State Responsibility), Third Report, Addendum (2000) A/CN.4/507/Add.2, para. 277 (2000).

[18] ARSIWA, *supra* note 2, at pt. I, ch. IV.

wrongful cyber operation. In addition, responsibility under Article 16 ARSIWA only arises if the assisting state was bound by the same obligation as the one that the assisted state breached.[19]

These strict requirements have been criticized as excessively narrow and not reflecting practice.[20] Further, it can be noted that specific regimes of international law which include provisions on aid or assistance tend to adopt lower thresholds. For instance, in the case law of the European Court of Human Rights, responsibility for aid or assistance to human rights violations can arise when the state "knew or ought to have known" that its assistance would contribute to a wrongful conduct.[21] A comparable threshold of constructive knowledge arguably applies to aid or assistance to serious violations of international humanitarian law.[22]

Whether aid or assistance to the cyber operation of another state can lead to joint and several liability is debatable. In situations of aid or assistance, the two states each commit a separate wrongful act, but their conduct together results in a harm for which reparation is sought. The ILC Commentaries affirm that "the assisting State will only be responsible to the extent that its own conduct has caused or contributed to the internationally wrongful act,"[23] and that "a State should not necessarily be held to indemnify the victim for all the consequences of the [main wrongful] act, but only for those which … flow from its own conduct."[24] Yet the ARSIWA provide no indication of possible criteria for such apportionment of responsibility. Interestingly, the ILC Commentaries mention that, when an injury is "effectively caused by a combination of factors, only one of which is to be ascribed to the responsible State, international practice and the decisions of international tribunals do not support the reduction or attenuation of reparation for concurrent causes."[25] A number of authors have also argued that an assisting state could be held jointly liable together with the main perpetrator, so that the assisting state could be required to provide reparation for the whole damage.[26] The argument is particularly strong when assistance constitutes a significant or necessary contribution to the main wrongful act.[27]

On the basis of the above, states providing aid or assistance to the cyber operation of another state can bear responsibility if they had actual—or possibly constructive—knowledge of the wrongful cyber operation. Further, states providing forms of assistance that are critical to the main cyber operation—for instance, an essential facility or unique technical expertise—could arguably bear joint and several liability for the damage caused by the cyber operation.

Lack of Due Diligence by a Territorial State

The third scenario analyzed in this essay is that of a state from whose territory another actor launches a cyber operation. The ICJ declared in the *Corfu Channel Case* that every state has an "obligation not to allow knowingly its

[19] ARSIWA Commentaries, *supra* note 2, at 65–67 (commentary to art. 16).

[20] Helmut Philipp Aust, Complicity and the Law of State Responsibility 377 (2011); Bernhard Graefrath, *Complicity in the Law of International Responsibility*, 2 Revue Belge Droit Int'l 371, 375 (1996); Vladyslav Lanovoy, *Complicity in an Internationally Wrongful Act*, *in* Principles of Shared Responsibility in International Law, *supra* note 5, at 152–61.

[21] El-Masri, *supra* note 3, at para. 198.

[22] Commentary on the First Geneva Convention para. 161 (Int'l Comm. of the Red Cross ed., 2d ed. 2016).

[23] ARSIWA Commentaries, *supra* note 2, at 66 (commentary to art.16(1)).

[24] *Id.* at 67 (commentary to art. 16(10)).

[25] *Id.* at 93 (commentary to art. 31(12)).

[26] Ian Brownlie, I System of the Law of Nations: State Responsibility 191 (1983); Graefrath, *supra* note 20, at 379; John Quigley, *Complicity in International Law: A New Direction in the Law of State Responsibility*, 57(1) Brit. Y.B. Int'l L. 77, 127 (1987).

[27] ARSIWA Commentaries, *supra* note 2, at 67 (commentary to art. 16(10)).

territory to be used for acts contrary to the rights of other States."[28] Locating the territorial origin of a cyber operation is not itself sufficient to attribute conduct to a state.[29] However, a territorial state can share responsibility in relation to the wrongful cyber operation of another state if it failed to take reasonable measures to ensure that its territory was not used by others for cyber operations. In particular, because cyber infrastructures are vulnerable to spoofing or hacking, states have an obligation of due diligence to ensure that infrastructure located in their territory is protected from covert use by other states.

As with aid or assistance, shared responsibility for lack of due diligence involves two distinct wrongful acts: the cyber operation itself and the territorial state's negligence that indirectly contributed to the realization of that operation. Cyber operations are not as such attributable to a negligent territorial state, but the failure to take action in circumstances where a state knows that its territory is used for a wrongful cyber operation engages its responsibility. The requirement of knowledge is satisfied also when the territorial state "must have known"[30] of its territory being used for wrongful cyber operations (constructive knowledge).

It would be difficult to argue that a territorial state should be liable to pay full reparation for damage caused by a cyber operation that it negligently let happen on its territory.[31] In circumstances where a territorial state is not merely negligent but also actively supports the cyber operation of another state, shared responsibility can be upheld under the framework of aid or assistance. This essay nonetheless takes the view that, depending on the degree of knowledge and good faith of a territorial state, a negligent failure could sometimes lead to an obligation of full reparation. For instance, if a territorial state has full knowledge of an ongoing cyber operation and remains inactive in addressing it, it could be argued that the territorial state is jointly liable with the main perpetrator.

Conclusion

In view of the difficulties in attributing cyber conduct to specific states, it is useful to identify when the responsibility of multiple states that are directly or indirectly implicated in a cyber operation can be engaged. Shared responsibility can allow victim states to identify the responsibility of more actors, without leading to a diffusion of responsibility. Indeed, as this essay argues, shared responsibility can entail an obligation of each responsible state to provide full reparation for the damage caused by the combination of wrongful acts.

In order to further clarify the conditions and consequences of shared responsibility, the SHARES Project has engaged in the process of drafting a set of Principles on Shared Responsibility in International Law. These Principles, expected to be finalized in 2019, will provide further guidance on the circumstances in which multiple states can be found responsible in relation to a cyber operation.

[28] Corfu Channel Case, (UK v. Alb.), 1949 ICJ Rep. 4, 22 (Apr. 9) [hereinafter Corfu Channel Case]. *See also* Tallinn Manual on the International Law Applicable to Cyber Warfare (Michael N. Schmitt ed., 2013), rule 5 [hereinafter Tallinn Manual].

[29] Tallinn Manual, *supra* note 27, at Rule 7.

[30] Corfu Channel Case, *supra* note 27, at 19.

[31] For a different view, see Luke Chircop, *A Due Diligence Standard of Attribution in Cyberspace*, 67 Int'l & Comp. L.Q. 643 (2018).