Complicity in Unlawful Offensive Cyber Operations Under International Law on State Responsibility

Samuli Haataja
Griffith Law School, Griffith University, Gold Coast, Australia

s.haataja@griffith.edu.au

Abstract: States are increasingly engaging in cybersecurity cooperation activities and providing support to other states in offensive cyber operations. While international cooperation is generally encouraged and many cybersecurity cooperation activities are lawful, there is also a risk of being complicit in the internationally wrongful acts of other states. This paper examines the risk of complicity in offensive cyber operations under international law on aiding or assisting. It argues that, while international law in this context applies to cyber operations by states, existing uncertainties and limitations around the key components of the law on aiding or assisting are compounded by competing interpretations about how international law generally applies to state conduct in cyberspace. The paper consists of four sections. Following the introduction in section one, section two outlines some of the ways in which states are cooperating in relation to cybersecurity and offensive cyber operations. Section three examines the key elements of international law on aiding or assisting as contained within article 16 of the International Law Commission's Articles on the Responsibility of States for Internationally Wrongful Acts, and the extent to which these apply or are problematised in relation cyber operations. It demonstrates that article 16 adopts a broad approach to what constitutes 'aiding or assisting' and this captures various types of activities in support of cyber operations provided the aid or assistance contributes significantly to a wrongful act of another state, the accomplice state has knowledge of the factual circumstances and the illegality of the act by the principal state, and where the accomplice state and principal state are bound by the same legal obligation. Section four concludes by outlining the limits of cooperation in the cyber context and how states can mitigate the risk of complicity in violations of international law.

Keywords: aid and assistance, cyber operations, international law, state responsibility

1. Introduction

This paper considers aiding or assisting in cyber operations under international law on state responsibility. It examines the risk of state complicity in violations of international law arising from cybersecurity cooperation. It argues that, while international law on aiding or assisting applies to cyber operations, existing uncertainties and limitations around the key elements of the law are compounded by competing interpretations about how international law generally applies to state conduct in cyberspace.

This paper consists of four sections. Section two outlines the various ways in which states are cooperating in relation to cybersecurity and cyber operations. Section three examines how international law on aiding or assisting, as contained in article 16 of the International Law Commission's (ILC) Articles on the Responsibility of States for Internationally Wrongful Acts (ARSIWA) (ILC 2001), applies to cyber operations. It demonstrates that article 16 covers a broad range of conduct and captures any form of aiding or assisting, whether this involves sharing mere lines of code, information about vulnerabilities, or malware provided there is a causal connection between the aid or assistance and the internationally wrongful act to which it contributes. However, the requirement under article 16 that the aiding or assisting state has knowledge of the circumstances of the wrongful conduct that they are contributing to is problematised by competing interpretations of how international law applies in cyberspace. Finally, the double obligation requirement within article 16 has potential to limit the application of the law in relation to regional cybersecurity treaties, and where states are persistent objectors to rules of customary international law in the cyber context. Section four provides a conclusion.

2. Cybersecurity and International Cooperation

States are increasingly cooperating in relation to cybersecurity activities and providing support to others engaging in cyber operations. For example, the recent AUKUS partnership between Australia, the United Kingdom (UK) and the United States (US) includes joint efforts to 'strengthen[] cyber capabilities' (White House 2022a) and Quad leaders have in 2022 agreed to 'strengthen information-sharing' among their Computer Emergency Response Teams (CERTs) (White House 2022b). The US also revealed it had conducted cyber operations in support of Ukraine in 2022 during its war with Russia. According to Paul Nakasone, this involved 'a series of operations across the full spectrum; offensive, defensive, [and] information operations' (Martin 2022). In the same context, it was noted that the US has been involved in sharing intelligence with its allies to undermine their adversaries' abilities to use their cyber capabilities (Martin 2022).

A number of states also discuss cooperation in their national positions on how international law applies to cyber operations. Canada, for example, in outlining its position on countermeasures, maintains that a state can provide assistance to another state requesting it where it 'does not possess all the technical … expertise to respond to internationally wrongful cyber acts' (Government of Canada 2022). Israel, in discussing the status of the due diligence principle, maintains that the nature of cyberspace 'incentivize[s] cooperation between States on a voluntary basis' and that CERTs regularly exchange information and cooperate to mitigate cybersecurity incidents (Schöndorf 2021, p. 404). As these examples and statements illustrate, states are cooperating in relation to different cyber activities and engaging in cyber operations in support of other states.

Cooperation around cybersecurity can involve a range of technical activities conducted for different purposes, many of which are lawful.[1] For example, states can share information about unknown vulnerabilities in software or hardware for the purpose of improving each others' cybersecurity. However, states can also share tools or techniques that exploit these vulnerabilities, and other malware utilising a range of exploits in order to obtain unauthorised access or disrupt the operation of adversary systems. Where these activities cause effects in the networks of another state, they can constitute violations of the international legal obligations of the state using these capabilities. However, there is also risk that the state involved in sharing these capabilities or providing technical support becomes complicit in violations of international law.

3. International Law on Aiding or Assisting

Under international law on state responsibility, a state (the accomplice state) can be responsible for aiding or assisting another state (the principal state) in an internationally wrongful act. Article 16 of the ARSIWA provides that:

> A State which aids or assists another State in the commission of an internationally wrongful act by the latter is internationally responsible for doing so if: (a) that State does so with knowledge of the circumstances of the internationally wrongful act; and (b) the act would be internationally wrongful if committed by that State. (ILC 2001)

This is echoed in the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Tallinn Manual) where rule 18(a) provides that, in relation to cyber operations, a state is responsible for:

> its aid or assistance to another State in the commission of an internationally wrongful act when the State provides the aid or assistance knowing of the circumstances of the internationally wrongful act and the act would be internationally wrongful if committed by it[.] (Schmitt 2017, p. 100)

Despite some debate about whether article 16 is a primary or secondary rule of international law (Jackson 2015, p. 149), the International Court of Justice has stated that it reflects customary international law on aiding or assisting (ICJ 2007, p. 217). Therefore, while cooperation among states is generally encouraged, article 16 provides the limits of acceptable conduct when doing so (Jackson 2015, p. 158). In other words, it defines the boundaries between lawful cooperation among states and complicity in unlawful conduct that in itself violates international law.

Article 16 consists of four components. First, it requires conduct by the accomplice state that constitutes 'aid or assistance' to the principal state. Second, there must be a causal connection or nexus between the aid or assistance provided by the accomplice state and the wrongful conduct by the principal state. Third, the accomplice state needs to have 'knowledge of the circumstances of the internationally wrongful act' by the principal state. Finally, under the 'double obligation' requirement in article 16(b), the accomplice state must be bound by the same legal obligation that is being violated by the principal state. Each of these will be examined in turn, including how they apply and the extent to which they are problematised in the cyber context.

[1] Passive cyber defense measures, such as the use of firewalls, applying patches to software and other measures that do not cause effects outside a state's own territory, generally do not infringe on other states' rights under international law (Lahmann 2020, p. 125).

3.1 'Aiding or Assisting'

Article 16 adopts a broad approach to activities and conduct that can constitute 'aiding or assisting.' While the ILC did not define aiding or assisting, it provided a number of examples of conduct that can amount to such including providing essential facilities, financial support, closing international waterways, facilitating abduction of persons, or assisting in the destruction of property (Crawford 2002, p. 148). Similarly, a survey of state practice in this context provides examples such as the provision of military support, assistance in unlawful uses of force, foreign aid and economic cooperation, shelter and safe haven for unlawful activities, legal assistance, and extradition (Aust 2011, p. 108). As these examples illustrate, the conduct that can constitute aiding or assisting under article 16 is broad. Others adopt a similar position (see Jackson 2015, p. 154; Crawford 2013, p. 402). Aust argues that it is not possible to provide definitive list of what constitutes 'aid or assistance' or abstract criteria to determine it, and that what constitutes 'aid or assistance' is to be determined on a case-by-case basis (Aust 2011, pp. 210, 230). Similarly, the Tallinn Manual experts maintained that states can be responsible for aiding or assisting whether the conduct is 'cyber or non-cyber in nature' (Schmitt 2017, p. 100). Nonetheless, aiding or assisting generally requires positive acts by the accomplice state meaning omissions are excluded (Crawford 2013, pp. 403-5), as are situations where states simply provide 'advice, encouragement or incitement' to another state (Crawford 1999, p. 48). Accordingly, article 16 adopts a broad approach under which any kind of aid or assistance in cybersecurity cooperation activities can potentially fall within its ambit.

3.2 Causal Connection

There must, however, be a causal connection or nexus between the aid or assistance by the accomplice state, and the wrongful act by the principal state. According to the ILC, the accomplice state will only be responsible 'to the extent that its own conduct has caused or contributed to the internationally wrongful act' (Crawford 2002, p. 148).

As to how to determine whether the causal connection is sufficient, the ILC maintained that the aid or assistance does not need to be 'essential to the performance of the wrongful act' provided it 'contributed significantly' to the principal state's wrongful act (Crawford 2002, p. 149). Jackson maintains this requires 'material facilitation' of the wrongful act, as it 'catches conduct with a sufficient link to another state's wrongdoing while excluding the incidental relationships that arise from virtually every state interaction' (Jackson 2015, p. 158). But the aid or assistance cannot be too remote or indirectly related to the wrongful act (Nolte & Aust 2009, p. 10.) Similarly, a 'but for' test is not appropriate because if the aid or assistance is essential to the performance of the wrongful act, then the accomplice state is more likely to the main author of the wrongful act or jointly responsible (ILC 2002, art. 47).

In the cyber context, the Tallinn Manual experts adopted a similar position, noting that 'irrespective of the form it takes, [the aid or assistance] must materially and causally contribute to the act' (Schmitt 2017, p. 102). They maintained that aiding or assisting is a threshold above involvement that is 'merely tangential' to the wrongful act, but below the threshold of 'jointly conducting' it (Schmitt 2017, p. 102). As an example of when the aid or assistance crosses the latter threshold, the Tallinn Manual described a situation where 'a State provides uniquely effective and indispensable decryption capabilities to another State to enable the latter to conduct a harmful cyber operation, and without which the operation could not be mounted' (Schmitt 2017, p. 102). Boutin similarly argues that where the aid or assistance is 'critical to the main cyber operation', such as where it involves 'an essential facility or unique technical expertise', then that could give rise to joint responsibility and rise above the threshold of aiding or assisting under article 16 (Boutin 2019, p. 200).

Accordingly, a broad range of cybersecurity cooperation activities, such as support in conducting cyber operations that constitute internationally wrongful acts, can constitute aiding or assisting. This can involve sharing information about unknown vulnerabilities or techniques on how to exploit vulnerabilities, or provision of malware designed to cause particular effects. In each instance, even where the aid or assistance is seemingly minor from a technical perspective (such information about an unknown vulnerability), provided that it contributes significantly to the commission of an internationally wrongful act by the principal state, then the activity can constitute 'aid or assistance' under article 16. This, however, can be difficult to determine in the cyber context. For example, in some circumstances information about a single unknown vulnerability may be an important factor in the development of malware used in a cyber operation against another state and contributes significantly to the wrongful act for which it is used. In other circumstances, such as where the cyber operation involves malware exploiting multiple unknown vulnerabilities or involves a range of different tools and techniques, then sharing information about how to exploit a single unknown vulnerability could only be an

incidental factor that is too indirect to the wrongful act that the malware is used for. Therefore, combined with the lack of precision in the threshold of when aiding or assisting contributes significantly to a wrongful act, establishing or demonstrating that cybersecurity cooperation activities have met this threshold can be difficult.

3.3 'Knowledge of the Circumstances'

The third component is the requirement under 16(a) that the accomplice state has 'knowledge of the circumstances of the internationally wrongful act' by the principal state. This includes actual knowledge but does not include constructive knowledge (Crawford 2013, p. 406). Some also maintain that this includes where there is 'wilful blindness' on behalf of the accomplice state (Jackson 2015; Moynihan 2016; Milanovic 2021). According to the commentary to the ILC articles, the accomplice state must be 'aware of the circumstances making the conduct of the assisted State internationally wrongful' (Crawford 2002, p. 149). This can be interpreted to mean that the accomplice state must have knowledge of both the factual circumstances and illegality of the conduct by the principal state (Moynihan 2016, pp. 11-1; Lanovoym 2016, p. 100).

However, there is a degree of uncertainty about whether 'knowledge of the circumstances of the internationally wrongful act' also requires intention on behalf of the accomplice state to aid or assist the principal state in the wrongful act, or whether knowledge is sufficient. This uncertainty arises because the ILC commentary provides that the aid or assistance by the accomplice state 'must be given with a view to facilitating the commission of the wrongful act' by the principal, and the commentary notes that accomplice state will not be responsible unless it 'intended, by the aid or assistance given, to facilitate the occurrence of the wrongful conduct' (Crawford 2002, p. 149). Further, the reference to intention in the commentary to article 16 is inconsistent with the approach to 'intent' that the ARSIWA generally adopt (Crawford 2002, p. 84; Nolte & Aust 2009, p. 13).

This uncertainty has given rise to some debate about whether or not article 16 requires a degree of intent by the accomplice state, or whether knowledge is sufficient (Jackson 2015, pp. 160-1). However, among those who do argue that intention is required in addition to knowledge (Crawford 2013, pp. 407-8; Aust 2011, pp 237-9; Moynihan 2016, pp. 18-9; Milanovic 2021, p. 1321), there is a tendency to adopt a broad or flexible approach to determining this. For example, Nolte and Aust emphasise the importance of intention but maintain that a flexible approach should be taken to prevent states from hiding behind the intent requirement, and that in some cases 'a lack of intent can be offset by sufficient knowledge' (Nolte & Aust 2009, p. 15). Crawford also maintains that intent can be imputed where the aid or assistance is provided 'with certain or near-certain knowledge as to the outcome' (Crawford 2013, p. 408). Similarly, Moynihan maintains that intention is required but concludes that this can be satisfied where the accomplice state has 'knowledge or virtual certainty that the recipient state will use the assistance unlawfully' Moynihan 2016, p. 20). Milanovic adopts a similar approach under which the accomplice state has 'indirect intent' where it chooses to provide aid or assistance in circumstances that it is 'practically certain' it would facilitate the commission of a wrongful act by the principal state (Milanovic 2021, p. 1321). Accordingly, even where article 16 is interpreted to require intention in addition to knowledge, most adopt a broad approach to determining this which highlights the importance of the accomplice state having knowledge in terms of a degree of certainty about factual circumstances and the illegality of the conduct in question.

In the cyber context, article 16's knowledge requirement is complicated by the competing interpretations about how international law applies to state activities as this affects whether the accomplice state has knowledge of the illegality of the conduct for which they are providing aid or assistance. For example, while most states agree that sovereignty operates as a rule of international law that can be violated, there continues to be uncertainty about the threshold at which a violation of sovereignty occurs (see Heller 2021, pp. 1458-64). Consider, for instance, where a state provides aid or assistance in the form of cyber capabilities that help the principal state to obtain unauthorised access to computers located within another state with the aim of taking down a botnet being operated from those systems. In this situation, the accomplice state may have knowledge of the relevant factual circumstances, but it may not have knowledge about the illegality of the conduct as it is unclear whether the principal state's conduct would violate sovereignty and be unlawful given the different positions that states have adopted to determining this.

3.4 The Double Obligation Requirement

The final component is the so called 'double obligation' requirement under article 16(b). This is based on the *pacta tertiis* rule (that treaties only create obligations to the parties to it, and not third parties) and requires that

the accomplice state and the principal state are bound by the same legal obligation that is being violated and that the accomplice state is aiding or assisting in (Crawford 1999, pp. 50-1).

The effect of the double obligation requirement is that it limits the scope of article 16. For example, in relation legal obligations arising from bilateral or regional treaties, states not party to these treaties may aid or assist in the breach of them without being responsible under article 16. Generally, in relation to obligations arising from customary international law, all states will be bound by the same obligation and satisfy the requirement in article 16(b). However, states that are persistent objectors and not bound by the general rule fall outside the scope of article 16(b) where they aid or assist in the wrongful act of another state (Jackson 2015, pp. 162, 167).

In the cyber context, an example of how the double obligation requirement may limit the application of article 16 arises from recent changes to European Union (EU) export controls over 'dual use' cyber capabilities (EU 2021). Under the new EU regulation, obligations are imposed on EU member states to limit to the export of dual use 'cyber-surveillance items' where they are or may be intended for use in connection with 'serious violations of human rights and international humanitarian law' (EU 2021, art. 5). In circumstances where a non-EU state aids or assists an EU member state in violations of the law, such as by contributing to the development of cyber-surveillance items with knowledge they will be exported, this would not be captured by article 16 given the requirement that both states are subject to the same legal obligation. While the EU regulation is not a regional treaty, it illustrates how there may be circumstances where a regional cybersecurity treaty only imposes obligations on certain states, and how the aid or assistance provided by those not party to the treaty would fall outside the scope of article 16.

Another example arises from persistent objectors to rules of customary international law. In 2020 NATO released its 'Allied Joint Doctrine for Cyberspace Operations' (AJP-3.20) in which its members expressed their agreement to a number of questions of how international law applies to cyber operations (NATO 2020). NATO's AJP-3.20 provides, for example, that cyber operations below the use of force threshold 'may nevertheless constitute a violation of international law as a breach of sovereignty' (NATO 2020, p. 20, fn. 26), and many states have expressed support for a similar position (see UN 2021). The UK, however, has since 2018 maintained that this is not the case, and this was reiterated in NATO's AJP-3.20 where the UK made a reservation to this effect (NATO 2020, p. v). Given that states have begun to carve out new understandings of how international law applies to their cyber activities (see Akande, Coco & Dias 2022, p. 24) and documents such as this can be regarded as evidencing state practice and *opinio juris* for this purpose, the UK's position can be interpreted as an effort to persistently object to the application of the rule of territorial sovereignty to cyber operations below the threshold of the non-intervention and non-use of force principles. In this context, and assuming a cyber specific rule on sovereignty develops into customary international law and that the UK would not be bound by this rule, then the application of article 16 is limited in relation to those persistent objectors. For example, where the UK were to aid and assist another state through the provision of cyber capabilities which contributed significantly to a cyber operation in violation of another state's sovereignty, the UK's conduct could fall outside the scope of article 16 given the double obligation requirement in article 16(b).

3.5 Article 16 and the Limits of Cooperation in the Cyber Context

Accordingly, article 16 adopts a broad approach to aiding or assisting which is neutral to the technologies used in this context. In relation to cybersecurity cooperation activities, the effect of this is that even where the provision of aid or assistance involves sharing lines of malicious code or information about unknown vulnerabilities, this can fall within the scope of article 16. But the key question is whether the aid or assistance by the accomplice state 'contributed significantly' to an internationally wrongful act by the principal state. This may be difficult to establish in the cyber context but will be considered on a spectrum. The aid or assistance must be more than 'merely tangential' participation (Schmitt 2017, p. 102) or an 'incidental factor' in the commission of the wrongful act (Crawford 2002, p. 151). But it must be less than 'essential to the performance of the wrongful act' or where the states are jointly conducting the wrongful act (Crawford 2002, p. 149; Aust 2011 pp. 212-3).

As to the requirement that the accomplice state has 'knowledge of the circumstances of the internationally wrongful act', the uncertainty around what extent of knowledge is required by the accomplice state is compounded in the cyber context. Essentially, while an accomplice state may have knowledge of the factual circumstances, it may be difficult to have knowledge of the illegality of the conduct by the principal state given that states have not yet reached consensus on how relevant primary rules of international law apply in the cyber context and the thresholds at which cyber operations will violate them (see UN 2021). Finally, the double

obligation requirement has potential to limit the scope of article 16 particularly in relation to obligations arising from regional treaties, and where states are persistent objectors to cyber specific rules of customary international law. This also demonstrates how debates about the status and scope of rules of international law in the cyber context, such as sovereignty, can have flow-on effects into other areas of law, such as aiding or assisting.

To mitigate the risk of complicity in internationally wrongful acts arising from cybersecurity cooperation activities, states should consider the circumstances surrounding the aid or assistance they are providing, and how the state they are aiding or assisting interprets international law to apply to cyber operations. Where there are concerns around the risk of complicity, the accomplice state can mitigate this by, for example, imposing conditions on the aid or assistance they provide (Moynihan 2016, pp. 38-44; Jackson 2015, p. 161). Further, given how the uncertainties in the law on aiding or assisting are compounded by debates about the status and scope of other rules of international law in the cyber context, it remains imperative for states to continue developing clarity about how they consider international law to apply in the cyber context, particularly in relation to rules such as sovereignty which can delineate the boundaries between lawful cyber espionage and unlawful cyber operations below the use of force threshold.[2]

4. Conclusion

This paper examined aiding or assisting in cyber operations under international law on state responsibility. It demonstrated how article 16 adopts a broad approach to what constitutes 'aiding or assisting' and how this captures various types of activities in support of cyber operations. While cybersecurity cooperation activities are generally lawful, there is a risk of complicity where the aid or assistance contributes significantly to a wrongful act of another state, the accomplice state has knowledge of the factual circumstances and the illegality of the act by the principal state, and where the accomplice state and principal state are bound by the same legal obligation. States can mitigate these risks by imposing conditions on the aid or assistance they provide, and by developing further clarity in their national positions on how international law, including the law on aiding or assisting, applies in the cyber context.

References

Akande, D, Coco, A, & Dias, TS 2022, 'Drawing the Cyber Baseline: The Applicability of Existing International Law to the Governance of Information and Communication Technologies', *International Law Studies*, vol. 99, pp 4-36.

Aust, HP 2011, *Complicity and the Law of State Responsibility*, Cambridge University Press, Cambridge.

Boutin, B 2019, 'Shared Responsibility for Cyber Operations', *AJIL Unbound*, vol. 113, pp 197-201, DOI:<https://doi.org/10.1017/aju.2019.31>.

Buchan, R 2019, *Cyber Espionage and International Law*, Hart, Oxford.

Crawford, J 1999, *Second Report on State Responsibility*, UN Doc A/CN.4/498.

Crawford, J 2002, *The International Law Commission's Articles on State Responsibility: Introduction, Text and Commentaries*, Cambridge University Press, Cambridge.

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

Delerue, F 2020, *Cyber Operations and International Law*, Cambridge University Press, Cambridge.

European Union (EU) 2021, Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast), 2021 OJ (L 206) 1.

Government of Canada 2022, *International law applicable in cyberspace*, 4 April, viewed 30 January 2023, <https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng>.

Heller, KJ 2021, 'In Defense of Pure Sovereignty in Cyberspace', *International Law Studies*, vol. 97, pp 1432-1499.

International Court of Justice (ICJ) 2007, *Case Concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia-Herzegovina v Yugoslavia)* (Judgment) [2007] ICJ Rep 43.

International Law Commission (ILC) 2001, *Responsibility of States for Internationally Wrongful Acts*, UNGA Res 56/83, 12 December, UN Doc A/RES/56/83.

Jackson, M 2015, *Complicity in International Law*, Oxford University Press, Oxford.

[2] Peacetime espionage is not directly addressed by international law and cyber espionage activities, depending on their effects, are generally not considered to violate international law (Schmitt 2017, p. 25). For those who argue that cyber espionage does violate international law on sovereignty, see, for example, Buchan (2019, p. 54) and Delerue (2020, p. 214).

Lahmann, H 2020, *Unilateral Remedies to Cyber Operations*, Cambridge University Press, Cambridge.
Lanovoym, V 2016, *Complicity and its Limits in the Law of International Responsibility*, Bloomsbury, Oxford.
Martin, A 2022, 'US military hackers conducting offensive operations in support of Ukraine, says head of Cyber Command', *Sky News*, 1 June 2022, viewed 30 January 2023, <https://news.sky.com/story/us-military-hackers-conducting-offensive-operations-in-support-of-ukraine-says-head-of-cyber-command-12625139>.
Milanovic, M 2021, 'Intelligence sharing in multinational military operations and complicity under international law', *International Law Studies*, vol. 97, pp 1269-1403.
Moynihan, H 2016, *Aiding and Assisting: Challenges in Armed Conflict and Counterterrorism*, Chatham House Research Paper, viewed 30 January 2023, <https://www.chathamhouse.org/sites/default/files/publications/research/2016-11-11-aiding-assisting-challenges-armed-conflict-moynihan.pdf>.
North Atlantic Treaty Organisation (NATO) 2020, *Allied Joint Doctrine for Cyberspace Operations, Allied Joint Publication-3.20*, NATO Standardisation Office, viewed 30 January 2023, <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf>.
Nolte, G & Aust, HP 2009, 'Equivocal Helpers—Complicit States, Mixed Messages and International Law' *International & Comparative Law Quarterly*, vol. 58, no. 1, pp 1-30, DOI:<https://doi.org/10.1017/S0020589308000821>.
Schmitt, M (ed.) 2017, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd edn, Cambridge University Press, Cambridge.
Schöndorf, R 2021 'Israel's Perspective on Key Legal and Practical Issues Concerning the Application International Law to Cyber Operations', *International Law Studies*, vol. 97, pp 395-406.
United Nations (UN) 2021, *Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266*, 13 July, UN Doc A/76/136*.
White House 2022a, *Fact Sheet: Implementation of the Australia – United Kingdom – United States Partnership (AUKUS)*, Press release, 5 April, viewed 30 January 2023, <https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/05/fact-sheet-implementation-of-the-australia-united-kingdom-united-states-partnership-aukus/>.
White House 2022b, *Fact Sheet: Quad Leaders' Tokyo Summit 2022*, 23 May, viewed 30 January 2023, <https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/23/fact-sheet-quad-leaders-tokyo-summit-2022/>.