The European Journal of International Law Vol. 33 no. 4

Not Illegal: The SolarWinds Incident and International Law

Kristen E. Eichensehr[*]

Abstract

In 2021, the USA and other governments formally blamed Russia for a wide-ranging hacking campaign that breached the update process for SolarWinds Orion network monitoring software and used that access to compromise numerous government agencies, companies and other entities. Despite denouncing Russia's cyber espionage and imposing sanctions, the USA did not call Russia's actions illegal as a matter of international law – and for good reason. Based on the publicly available facts, this article argues that the SolarWinds incident likely did not run afoul of international law as it currently stands. The article considers the prohibitions on the use of force and intervention, emerging rules with respect to violations of sovereignty and due diligence, and international human rights law, and it concludes with some reflections on the role of states and scholars in decisions about whether to close gaps in international law.

1 Introduction

The cyber-security incident known as SolarWinds first came to light on 8 December 2020 when cyber-security firm FireEye announced that it had been breached by a 'highly sophisticated state-sponsored attacker utilizing novel techniques'.[1] In the

[*] Martha Lubin Karsh and Bruce A. Karsh Bicentennial Professor, University of Virginia School of Law, Charlottesville, VA, USA. Email: keichensehr@law.virginia.edu. Thanks to Ashley Deeks, Richard Re and Michael Schmitt for helpful comments and to Joshua Goland and Denny Phane for excellent research assistance.

For an opposing view, see Coco, Dias and van Benthem, 'Illegal: The SolarWinds Hack under International Law', 33 *European Journal of International Law* (2022) 1275, available at https://doi.org/10.1093/ejil/chac063.

[1] K. Mandia, 'FireEye Shares Details of Recent Cyber Attack, Actions to Protect Community', *FireEye* (8 December 2020), available at https://web.archive.org/web/20220223175256/https://www.fireeye.com/blog/products-and-services/2020/12/fireeye-shares-details-of-recent-cyber-attack-actions-to-protect-community.html.

subsequent days, it became clear that FireEye was just one victim of a months-long Russian government operation that compromised the update process for network-monitoring software sold by SolarWinds, a Texas company, to breach numerous US government agencies, companies and others around the world.[2] The hacking campaign that the US government called 'an intelligence gathering effort'[3] and that one cyber-security expert more bluntly deemed 'one of the most effective cyber-espionage campaigns of all time'[4] roiled victims for months and resulted in the USA sanctioning Russia.

The SolarWinds incident violated US law,[5] but did it also violate international law? This article considers established and emerging legal rules and concludes, based on the publicly available facts, that SolarWinds likely did not run afoul of international law as it currently stands.[6] The article closes with some reflections on the role of states and scholars in the ongoing debates about the scope of international law governing cyber operations.

2 The SolarWinds Incident and States' Responses

The SolarWinds incident began with a supply chain hack: Russian government hackers compromised the update process for SolarWinds' Orion network-monitoring software and caused 18,000 of the company's customers to download an update containing malicious code.[7] The hackers then selected a smaller number of the breached entities for additional targeting,[8] using their initial access via Orion to reach the

2 See, e.g., E. Nakashima and C. Timberg, 'Russian Government Hackers Are Behind a Broad Espionage Campaign That Has Compromised U.S. Agencies, Including Treasury and Commerce', *Washington Post* (14 December 2020), available at www.washingtonpost.com/national-security/russian-government-spies-are-behind-a-broad-hacking-campaign-that-has-breached-us-agencies-and-a-top-cyber-firm/2020/12/13/d5a53b88-3d7d-11eb-9453-fc36ba051781_story.html.

3 Joint Statement by the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the Office of the Director of National Intelligence (ODNI), and the National Security Agency (NSA), 5 January 2021, available at www.cisa.gov/news/2021/01/05/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure.

4 D. Temple-Raston, 'A "Worst Nightmare" Cyberattack: The Untold Story of the SolarWinds Hack', *National Public Radio* (16 April 2021), available at www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack (quoting Stanford University's Alex Stamos).

5 See 18 U.S.C. § 1030.

6 I am not the first to reach this conclusion. See, e.g., D.P. Fidler, 'SolarWinds and Microsoft Exchange: Hacks Wrapped in a Cybersecurity Dilemma inside a Cyberspace Crisis', *Georgetown Journal of International Affairs* (12 April 2021), available at https://gjia.georgetown.edu/2021/04/12/solarwinds-and-microsoft-exchange-hacks-wrapped-in-a-cybersecurity-dilemma-inside-a-cyberspace-crisis; J. Goldsmith, 'Self-Delusion on the Russia Hack', *The Dispatch* (18 December 2020), available at https://thedispatch.com/p/self-delusion-on-the-russia-hack; M.N. Schmitt, 'Top Expert Backgrounder: Russia's SolarWinds Operation and International Law', *Just Security* (21 December 2020), available at www.justsecurity.org/73946/russias-solarwinds-operation-and-international-law/.

7 Temple-Raston, *supra* note 4.

8 D. Alperovitch and I. Ward, 'How Should the U.S. Respond to the SolarWinds and Microsoft Exchange Hacks?', *Lawfare* (12 March 2021), available at www.lawfareblog.com/how-should-us-respond-solarwinds-and-microsoft-exchange-hacks (noting that 'Russia opted not to exploit the vast majority of the networks it gained access to' and 'sent a kill switch to 99 percent of their potential victims, permanently disabling Russia's access').

organizations' Microsoft 365 cloud environments and the information therein.[9] US officials ultimately assessed that '9 federal agencies and about 100 private sector companies' suffered such advanced intrusions.[10]

The US government's response rolled out over several months. The US Cybersecurity and Infrastructure Security Agency immediately issued an emergency directive instructing US government agencies to disconnect devices affected by the compromise and later provided guidance on reinstalling updated versions of SolarWinds Orion, along with other actions to harden systems against further intrusions.[11] On 15 April 2021, the USA attributed 'the broad-scope cyber espionage campaign that exploited the SolarWinds Orion platform and other information technology infrastructures' to Russia's Foreign Intelligence Service (SVR in Russian) and imposed sanctions on Russia's intelligence services, including the SVR, as well as certain Russian companies that support those intelligence services.[12] In explaining the sanctions, the White House highlighted the wide scope of the intrusion, which gave the SVR 'the ability to spy on or potentially disrupt more than 16,000 computer systems worldwide', and the 'undue burden on the mostly private sector victims who must bear the unusually high cost of mitigating this incident'.[13] Pointing to 'Russia's history of… reckless and disruptive cyber operations', the US Treasury Department emphasized that '[t]he SVR has put at risk the global technology supply chain' and caused victims to spend 'millions of dollars' in remediation.[14]

However, the USA did not call the hack a violation of international law. Neither did numerous US allies, including Australia, Canada, the European Union and the United Kingdom (UK), all of which confirmed the attribution and condemned Russia's behaviour as malicious, destabilizing or malign.[15] The absence of states labelling the

[9] See R. Chesney, 'SolarWinds and the Holiday Bear Campaign: A Case Study for the Classroom', *Lawfare* (25 August 2021), available at www.lawfareblog.com/solarwinds-and-holiday-bear-campaign-case-study-classroom.

[10] 'Press Briefing by Press Secretary Jen Psaki and Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger', *White House* (17 February 2021), available at www.whitehouse.gov/briefing-room/press-briefings/2021/02/17/press-briefing-by-press-secretary-jen-psaki-and-deputy-national-security-advisor-for-cyber-and-emerging-technology-anne-neuberger-february-17-2021/.

[11] 'Emergency Directive 21-01 Mitigate SolarWinds Orion Code Compromise', *US Cybersecurity and Infrastructure Security Agency* (13 December 2020), available at www.cisa.gov/emergency-directive-21-01; Supplemental Guidance v3, *US Cybersecurity and Infrastructure Security Agency* (6 January 2021), available at https://www.cisa.gov/emergency-directive-21-01.

[12] 'Fact Sheet: Imposing Costs for Harmful Foreign Activities by the Russian Government', *White House* (15 April 2021), available at www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/; 'Treasury Sanctions Russia with Sweeping New Sanctions Authority', *US Department of the Treasury* (15 April 2021), available at https://home.treasury.gov/news/press-releases/jy0127.

[13] 'Fact Sheet', *supra* note 12.

[14] 'Treasury Sanctions Russia', *supra* note 12.

[15] See, e.g., Hon. M. Payne, Hon. P. Dutton MP and Hon. K. Andrews MP, 'Attribution of Cyber Incident to Russia', *Minister for Foreign Affairs* (15 April 2021), available at www.foreignminister.gov.au/minister/marise-payne/media-release/attribution-cyber-incident-russia; 'Statement on SolarWinds Cyber Compromise', *Global Affairs Canada*, 15 April 2021, available at www.canada.ca/en/global-affairs/news/2021/04/statement-on-solarwinds-cyber-compromise.html; 'Declaration

SolarWinds intrusion an international law violation is not dispositive of whether the incident violated international law. A state that suffers an internationally wrongful act has no obligation to acknowledge that the act occurred or to identify the act as legally wrongful unless it intends to take countermeasures in response, which the USA did not.[16] Nonetheless, the fact that none of the states that condemned Russia's behaviour did so as a legal matter is probative because state practice and *opinio juris* determine the customary international law that governs state behaviour. In analysing whether Russia's SolarWinds intrusion violated international law, the next section therefore relies heavily on states' publicly proffered legal views.

3 Possible Legal Violations

As far as is publicly known, the SolarWinds intrusion involved a supply chain compromise by Russia to install malicious software into US government and other critical infrastructure entities for the purpose of espionage. Law and espionage have a complicated relationship. Although states criminalize spying in their domestic laws, international law is silent on espionage as such, and states have a long-standing practice of spying on one another. The common understanding is that 'international law either fails to regulate spying or affirmatively permits it'.[17] At the same time, deeming an operation espionage is not a *carte blanche*. A cyber operation intended to facilitate espionage could still violate international law depending on how it is conducted.[18] This section considers whether the SolarWinds incident violated international law prohibitions on the use of force and intervention or emergent rules on sovereignty and due diligence. It concludes with a brief word about international human rights law.

---

by the High Representative on Behalf of the European Union Expressing Solidarity with the United States on the Impact of the SolarWinds Cyber Operation', *Council of the European Union* (15 April 2021), available at www.consilium.europa.eu/en/press/press-releases/2021/04/15/declaration-by-the-high-representative-on-behalf-of-the-european-union-expressing-solidarity-with-the-united-states-on-the-impact-of-the-solarwinds-cyber-operation; 'North Atlantic Council Statement Following the Announcement by the United States of Actions with Regard to Russia', *North Atlantic Treaty Organization* (15 April 2021), available at www.nato.int/cps/en/natohq/official_texts_183168.htm; 'Russia: UK and US Expose Global Campaign of Malign Activity by Russian Intelligence Services', *UK Government* (15 April 2021), available at www.gov.uk/government/news/russia-uk-and-us-expose-global-campaigns-of-malign-activity-by-russian-intelligence-services.

16 See Eichensehr, 'Defend Forward and Attribution', in J. Goldsmith (ed.), *The United States' Defend Forward Cyber Strategy: A Comprehensive Legal Assessment* (2022) 260, at 262–264.

17 See, e.g., Deeks, 'An International Legal Framework for Surveillance', 55 *Virginia Journal of International Law* (2015) 291, at 300; see also M.N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2017), at 169 (hereinafter *Tallinn Manual 2.0*) ('customary international law does not prohibit espionage *per se*').

18 See *Tallinn Manual 2.0*, *supra* note 17, at 170 (whether a cyber-espionage operation is lawful 'depends on whether the way in which the operation is carried out violates any international law obligations that bind the State'). The SolarWinds operation may well have violated international norms of responsible behaviour in cyberspace. See Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security (hereinafter 2021 GGE Report), UN Doc. A/76/135, 14 July 2021, at 8–17.

A *Prohibition on the Use of Force*

The SolarWinds incident did not constitute a use of force in violation of Article 2(4) of the Charter of the United Nations and customary international law. Building on the International Court of Justice's (ICJ) analysis in the *Nicaragua* case,[19] states are coalescing around the position that a cyber operation that is similar in 'scale and effects' to a non-cyber use of force will be considered a use of force.[20] The USA has explained that, '[i]f the physical consequences of a cyber activity result in the kind of damage that dropping a bomb or firing a missile would, that cyber activity should equally be considered a use of force/armed attack'.[21] The SolarWinds incident does not meet this threshold: it did not cause death, injury, destruction or even the sort of very significant non-physical disruption that some states might consider to meet the scale and effects test.[22]

B *Prohibition on Intervention*

Cyber operations that do not constitute uses of force might nonetheless run afoul of the customary international law prohibition on intervention.[23] The existence of the prohibition on intervention is well settled, but its scope with respect to cyber operations is not.[24] In the *Nicaragua* case, the ICJ explained that '[t]he principle of non-intervention involves the right of every sovereign State to conduct its affairs

[19] *Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States)*, Judgment, 27 June 1986, ICJ Reports (1986) 14, para. 195.

[20] See, e.g., 'International Law Applicable in Cyberspace', *Government of Canada* (22 April 2022), para. 45, available at www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng#a12; 'Position Paper on the Application of International Law in Cyberspace', *Germany Federal Government* (2021), at 6, available at www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf; *Tallinn Manual 2.0*, *supra* note 17, at 330.

[21] United Nations General Assembly, 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 Government 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 (hereinafter GGE Compendium), UN Doc. A/76/136, 13 July 2021, at 137, available at front.un-arm.org/wp-content/uploads/2021/08/A-76-136-EN.pdf (USA) (last visited 10 November 2022).

[22] See *ibid.*, at 58 (Netherlands) ('at this time it cannot be ruled out that a cyber operation with a very serious financial or economic impact may qualify as the use of force'); Schmitt, *supra* note 6 (SolarWinds' effects 'are not at the level that any state has even hinted might justify characterization as a use of force'). But see D.B. Hollis and T. van Bentham, 'What Would Happen If States Started Looking at Cyber Operations as a "Threat" to Use Force?', *Lawfare* (30 March 2021), available at www.lawfareblog.com/what-would-happen-if-states-started-looking-cyber-operations-threat-use-force.

[23] *Nicaragua*, *supra* note 19, para. 202.

[24] See, e.g., GGE Compendium, *supra* note 21, at 57 (Netherlands) ('[t]he precise definition of coercion, and thus of unauthorised intervention, has not yet fully crystallised in international law'); *ibid.*, at 116 (United Kingdom) (describing 'the precise boundaries of' the prohibition on intervention as 'the subject of on-going debate'); 'International Law Applicable in Cyberspace', *Government of Canada*, *supra* note 20, para. 25 ('further State practice and *opinio juris* will help clarify the thresholds for the rule of non-intervention, and the scope of customary law in this area over time').

without outside interference'.[25] Intervention has two elements: (i) it must 'bear[] on matters in which each State is permitted… to decide freely', including 'the choice of a political, economic, social and cultural system, and the formulation of foreign policy', and (ii) it must involve 'coercion in regard to such choices, which must remain free ones'.[26] The first element is often described as involving a state's *domaine réservé*,[27] and it is somewhat clearer than the second element – coercion – which 'is not defined in international law'.[28]

Although the SolarWinds incident arguably interfered with the US *domaine réservé*, given the compromises of numerous US government departments, it did not coerce the USA and thus does not constitute intervention. The *Tallinn Manual* explains that coercion generally 'refers to an affirmative act designed to deprive another State of its freedom of choice, that is, to force that State to act in an involuntary manner or involuntarily refrain from acting in a particular way' with respect to its internal or external affairs.[29] Upon discovering the intrusion, the USA cut off Russia's access to compromised systems by disconnecting devices using the SolarWinds software and directing the updating and reinstallation of the software, and it subsequently invested in cybersecurity upgrades. But basic responses to the discovery of espionage and attempts to prevent its recurrence do not equate to a denial of freedom of choice.

Moreover, there is no evidence that Russia intended to coerce the USA, as many believe is required for intervention.[30] Simply put, spying on a state to discern what actions it is likely to take is not the same as coercing it to take, or to refrain from, any particular action.[31] The US efforts to stop the espionage and harden systems against recurrence suggest either a lack of intended coercion or that whatever coercion might have been intended failed spectacularly, resulting in improved defences that were counterproductive to Russia's espionage aims.

SolarWinds is also unlike examples that states have given of prohibited interventions. Prominent among such examples is cyber operations 'to prevent another State from holding an election, or manipulate the electoral system to alter the results of an election in another State'.[32] Other frequent examples include interfering with the

[25] *Nicaragua*, *supra* note 19, para. 202.

[26] *Ibid.*, para. 205.

[27] See, e.g., GGE Compendium, *supra* note 21, at 34 (Germany).

[28] *Tallinn Manual 2.0*, *supra* note 17, at 317.

[29] *Ibid.*

[30] See, e.g., GGE Compendium, *supra* note 21, at 34 (Germany); *ibid.*, at 57 (Netherlands); *Tallinn Manual 2.0*, *supra* note 17, at 317, 321.

[31] See, e.g., *Tallinn Manual 2.0*, *supra* note 17, at 323 ('[c]yber espionage *per se*, as distinct from the underlying acts that enable the espionage,… does not qualify as intervention because it lacks a coercive element'); Rt. Hon. S. Braverman, 'International Law in Future Frontiers', *UK Government* (19 May 2022), available at www.gov.uk/government/speeches/international-law-in-future-frontiers ('[i]t is this coercive element that most obviously distinguishes an intervention prohibited under international law from, for example, more routine and legitimate information-gathering and influencing activities that States carry out as part of international relations').

[32] GGE Compendium, *supra* note 21, at 5 (Australia). For similar views, see *ibid.*, at 34 (Germany); *ibid.*, at 69 (Norway); *ibid.*, at 116–117 (United Kingdom); *ibid.*, at 140 (USA); 'International Law Applicable in Cyberspace', *Government of Canada*, *supra* note 20, at para. 24; 'The Application of International Law to

operations of a state's legislature,[33] disrupting provision of health care[34] and significantly disrupting a state's financial system or other critical infrastructure.[35] All of these examples involve disruptions with more significant direct consequences for governments or individuals than the compromise of information involved in SolarWinds.

C *Violation of Sovereignty*

Whether cyber operations below the use of force threshold and outside of prohibited intervention violate international law has become a hotly contested issue. In 2017, the *Tallinn Manual 2.0* controversially took the position that sovereignty is a standalone rule of international law, such that violations of a state's sovereignty constitute an internationally wrongful act.[36] A number of states have subsequently endorsed this view, though often with the caveat that only operations above a certain threshold constitute violations. For example, Germany specified that 'negligible physical effects and functional impairments below a certain impact threshold' do not violate sovereignty.[37] On the other side of the spectrum, the UK has rejected the existence of a standalone rule of sovereignty, framing sovereignty as a principle of international law that informs other rules like non-intervention, but denying that states 'can currently extrapolate from that general principle a specific rule or additional prohibition for cyber activity beyond that of a prohibited intervention'.[38]

The US position on the question has been ambiguous. A 2020 speech by the US Defense Department's General Counsel suggested that the US view 'shares similarities with' the UK position.[39] In a 2021 filing with the United Nations Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (GGE), however, the USA explained that 'one State's non-consensual cyber operation in another State's territory, even if it falls below the threshold of a use of force or non-intervention, could also violate international law', but does 'not constitute a *per se* violation of international law', a distinction that 'is perhaps most clear where such activities in another State's territory have no effects or *de minimis* effects'.[40] Given divergences among states about the existence

State Activity in Cyberspace', *New Zealand Government* (1 December 2022), para. 10, available at https://dpmc.govt.nz/sites/default/files/2020-12/The%20Application%20of%20International%20Law%20to%20State%20Activity%20in%20Cyberspace.pdf.

33 See, e.g., GGE Compendium, *supra* note 21, at 5 (Australia).

34 *Ibid.*, at 116-17 (United Kingdom); *ibid.*, at 140 (USA).

35 See, e.g., *ibid.*, at 5 (Australia); *ibid.*, at 69 (Norway); *ibid.*, at 116–117 (United Kingdom); 'International Law Applicable in Cyberspace', *Government of Canada*, *supra* note 20, para. 24; 'Application of International Law', *New Zealand Government*, *supra* note 32, para. 10.

36 *Tallinn Manual 2.0*, *supra* note 17, at 17–27.

37 'Position Paper', *Germany Federal Government*, *supra* note 20, at 4 (emphasis omitted).

38 Rt. Hon. J. Wright, 'Cyber and International Law in the 21st Century', *UK Government* (23 May 2018), available at www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century. The United Kingdom reaffirmed this position in May 2022. Braverman, *supra* note 31.

39 P.C. Ney Jr., 'DOD General Counsel Remarks at U.S. Cyber Command Legal Conference', *US Department of Defense* (2 March 2020), available at www.defense.gov/News/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/.

40 GGE Compendium, *supra* note 21, at 140 (USA).

of, and threshold for, a rule of sovereignty, even states that endorse the rule have acknowledged that 'further state practice is required for the precise boundaries of [sovereignty's] application to crystallise'.[41]

Even assuming that sovereignty is a rule, it does not appear that the SolarWinds incident violated it. The *Tallinn Manual* suggests that a sovereignty violation can occur via a breach of a state's territorial integrity or an 'interference with or usurpation of inherently governmental functions'.[42] With respect to territorial integrity, the *Tallinn Manual*'s experts agreed that cyber operations causing physical damage or injury or a loss of functionality necessitating 'repair or replacement of physical components of cyber infrastructure' would violate sovereignty.[43] SolarWinds did neither of these things and instead required the reinstallation of updated software. Only some *Tallinn Manual* drafters thought that a loss of functionality requiring software reinstallation would violate sovereignty, and the manual warns that additional state practice is needed to clarify when a loss of functionality violates sovereignty.[44] Notably, at least one sovereignty-as-a-rule state has said that 'cyber activity that requires rebooting or the reinstallation of an operating system is likely not a violation of territorial sovereignty'.[45]

Turning to the second proposed basis, SolarWinds targeted inherently governmental functions, but whether it interfered with or usurped them is a separate question. Michael Schmitt, the *Tallinn Manual*'s editor and a leading proponent of the sovereignty-as-a-rule position, answered the question in the negative, arguing that 'the mere fact of espionage has never been characterized as interference, at least not as that concept is understood with respect to sovereignty violation'.[46] The confidentiality breaches caused by SolarWinds are a far cry from examples that states have given of interference with government functions, examples like 'altering or deleting data or blocking digital communication between public bodies and citizens so as to interfere with the delivery of social services, the conduct of elections, the collection of taxes, or the performance of key national defence activities'.[47]

Concluding that SolarWinds violated international law because it violated US sovereignty would require adopting not just the contested sovereignty-as-a-rule view but also a broad understanding of that position, which is not supported by state practice and *opinio juris*. The sovereignty violation question must also be considered in conjunction with some sovereignty-as-a-rule states' explicit view that cyber espionage does not violate sovereignty.[48] Such views would make little sense if efforts like

41 'Application of International Law', *New Zealand Government*, *supra* note 32, para. 12; see also GGE Compendium, *supra* note 21, at 68 (Norway).

42 *Tallinn Manual 2.0*, *supra* note 17, at 20.

43 *Ibid.*, at 20–21.

44 *Ibid.*, at 21.

45 'International Law Applicable in Cyberspace', *Government of Canada*, *supra* note 20, para. 17.

46 Schmitt, *supra* note 6.

47 GGE Compendium, *supra* note 21, at 68 (Norway).

48 See, e.g., 'International Law Applicable in Cyberspace', *Government of Canada*, *supra* note 20, para. 17 ('some cyber activities, such as cyber espionage, do not amount to a breach of territorial sovereignty, and hence to a violation of international law').

reinstalling software to block ongoing espionage transformed cyber espionage into a sovereignty violation.[49]

D *Due Diligence*

Some commentators have suggested that Russia's failure to prevent the SolarWinds incident might have violated an international law requirement of due diligence.[50] Due diligence is a long-standing concept in international law that requires a state to act to prevent or remedy transboundary harm emanating from its territory. In the *Corfu Channel* case, the ICJ identified 'every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States'.[51] Despite the due diligence principle's long pedigree, there are legal and factual difficulties with applying it to SolarWinds. Most fundamentally, states hold divergent views about whether or how due diligence applies to cyber operations.[52] States in the GGE have endorsed a norm of due diligence,[53] but prominent states including the UK and the USA have denied that it is legally binding.[54] Even states that endorse a legal rule of due diligence applied to cyber operations recognize that there is disagreement about its application.[55]

Even assuming the existence of a customary international law rule – a highly contested assumption – SolarWinds likely does not violate Russia's due diligence obligations for several reasons. Due diligence is framed as the responsibility of a territorial state to prevent another state or non-state actor from using its territory to cause harm to a victim state. As the *Tallinn Manual* explains, the due diligence rule 'assumes the involvement of at least three parties: (1) the target State of the cyber operation; (2) the territorial State that is the subject of the Rule, and (3) a third party that is the author of the cyber operation'.[56] In SolarWinds, however, there was no third party; the perpetrator was the Russian government. It is passing

[49] Cf. Schmitt, *supra* note 6 ('[f]inding a sovereignty breach on the basis that if the espionage is discovered, the victim state would decide to replace the affected infrastructure would be quite a stretch even for those who support sovereignty as a rule').

[50] Coco, Dias and van Benthem, 'Illegal: The SolarWinds Hack under International Law', 33 *European Journal of International Law* (2022) 1275.

[51] *The Corfu Channel Case (United Kingdom v. Albania)*, Judgment, 9 April 1949, ICJ Reports (1949) 4, at 22.

[52] See, e.g., D.B. Hollis, Improving Transparency: International Law and State Cyber Operations: Fourth Report, Doc. CJI/doc.603/20rev.1corr.1, in Organization of American States, *Annual Report of the Inter-American Juridical Committee to the General Assembly* (2020) 120, para. 57 ('there are competing views on whether due diligence is a requirement of international law in cyberspace').

[53] 2021 GGE Report, *supra* note 18, at 10 ('Norm 13(c) States should not knowingly allow their territory to be used for internationally wrongful acts using [information and communications technologies]').

[54] GGE Compendium, *supra* note 21, at 117 (United Kingdom); *ibid.*, at 141 (USA); see also 'Application of International Law', *New Zealand Government*, *supra* note 32, para. 17.

[55] See, e.g., GGE Compendium, *supra* note 21, at 48 (Japan); *ibid.*, at 58 (Netherlands).

[56] *Tallinn Manual 2.0*, *supra* note 17, at 32. The GGE report's description of a due diligence norm similarly suggests that 'a State should not permit *another State or non-State actor* to use ICTs within its territory to commit internationally wrongful acts'. 2021 GGE Report, *supra* note 18, para. 29 (emphasis added); see

strange to say that Russia violated its due diligence obligation by failing to stop its own conduct.[57]

Moreover, due diligence obligations are triggered when cyber operations cause some amount of harm contrary to the rights of the targeted state.[58] States and commentators have interpreted this element to require that the victim state suffer an internationally wrongful act or what would be an internationally wrongful act if done by a state.[59] Finding a violation of due diligence therefore depends on identifying some other violation of international law – a criterion not clearly met for SolarWinds.

E *International Human Rights Law*

In the past decade, states have recognized that international human rights law applies to cyber activities and, in particular, that 'the same rights that people have offline must also be protected online, including the right to privacy'.[60] As a matter of both customary and treaty law, however, there are jurisdictional limits on states' human rights obligations that become important in the context of cross-border cyber operations.[61] For example, even those who endorse a broad understanding of the International Covenant on Civil and Political Rights 'concede that a state party has obligations only to those individuals in territory under that state's "effective control" (the spatial model of jurisdiction) or who are subject to that state's legal jurisdiction (the personal model of jurisdiction)'.[62] Similarly, the majority of the *Tallinn Manual* drafters concluded that 'physical control over territory or the individual is required before human rights law obligations are triggered' and that 'the premise of exercising power or effective control by virtual means such that human rights obligations attach runs contrary to both extensive State practice and the paucity of expressions of *opinio juris* thereon'.[63]

also GGE Compendium, *supra* note 21, at 76 (Romania) (noting that due diligence involves acts by 'a non-State actor or a third State… from or through the territory of the potentially responsible State').

57 Due diligence fits more naturally in the context of criminal ransomware emanating from Russia. See Oxford Institute for Ethics, Law and Armed Conflict, 'The Oxford Statement on International Law Protections in Cyberspace: The Regulation of Ransomware Operations', para. 4, available at www.elac.ox.ac.uk/the-oxford-process/the-statements-overview/the-oxford-statement-on-ransomware-operations/.

58 See *Tallinn Manual 2.0*, *supra* note 17, at 34; but see *ibid.*, at 36 ('[t]he precise threshold of harm at which the due diligence principle applies is unsettled in international law'); Jensen and Watts, 'Due Diligence and Defend Forward', in J. Goldsmith (ed.), *The United States' Defend Forward Cyber Strategy: A Comprehensive Legal Assessment* (2022) 236, at 237 ('the precise threshold or degree of harm required to establish a breach remains unsettled').

59 See, e.g., GGE Compendium, *supra* note 21, at 7 (Australia); 2021 GGE Report, *supra* note 18, para. 29 (emphasis added) (describing a norm requiring states to act 'if a State is aware of or is notified in good faith that *an internationally wrongful act* conducted using ICTs is emanating from or transiting through its territory'); *Tallinn Manual 2.0*, *supra* note 17, at 34.

60 E.g. UN Human Rights Council, The Right to Privacy in the Digital Age, UN Doc. A/HRC/Res/42/15, 7 October 2019, para. 4.

61 See *Tallinn Manual 2.0*, *supra* note 17, at 182–186.

62 Deeks, *supra* note 17, at 308; see also International Covenant on Civil and Political Rights 1966, 999 UNTS 171.

63 *Tallinn Manual 2.0*, *supra* note 17, at 185; *cf.* 'Application of International Law', *New Zealand Government*, *supra* note 32, at 4 ('[t]he circumstances in which states exercise jurisdiction, through cyber means, over individuals outside their territory is currently unsettled').

Even assuming that the SolarWinds incident infringed victims' privacy or other rights, the jurisdictional limitations on international human rights law render it unlikely that Russia was obliged to respect the rights of the victims affected by the compromise. There is a separate question about whether states in which victims were located, particularly the USA, failed in an obligation to protect the human rights of victims in their territory. Nonetheless, even as to that question, states disagree in general about the scope of a state's duty to protect,[64] and what such a duty would require with respect to defending against foreign cyber espionage is unclear, particularly given divergences in states' domestic approaches to cyber-security regulation. The 2021 GGE report included a norm that 'States should take appropriate measures to protect their critical infrastructure from' cyber threats, but it stopped short of mandating such measures and left room for wide variation.[65] Cyber operations can certainly violate international human rights law, but it is far from clear that SolarWinds did so.

4 Conclusion

The SolarWinds incident was disruptive and costly for the victims, both in terms of remediation costs and the harder-to-quantify harms from stolen information. In some ways, it is deeply unsatisfying to conclude that international law does not clearly prohibit and may even permit such operations. At the same time, it is important to be clear about why that is the case. Cyber operations are putting pressure on international law, revealing the gaps that exist and that states may choose to fill with new rules, like a violation of sovereignty, or broader interpretations of existing rules, like the prohibition on intervention. But states may also choose not to close all of the gaps. Just as international law has long tolerated espionage, states may similarly leave cyber espionage and other operations below the use-of-force level at least partly unregulated, prioritizing flexibility over tamping down such behaviours. The state practice and *opinio juris* elements ensure that the establishment of customary international law remains the prerogative of states.

The legal debates about international law and cyberspace have come a long way in the decade since the 2013 GGE report cryptically confirmed that international law applies to cyberspace.[66] Increasing numbers of states are providing thoughtful and detailed positions about cyber and international law in venues like the GGE and the Organization of American States and in speeches and position papers. As the sophistication of discussions increases, scholars and other commentators also have roles

[64] See *Tallinn Manual 2.0*, *supra* note 17, at 197, n. 433 (noting that states, including the USA and the United Kingdom, 'hold the position that the obligation to protect is limited and cannot be characterized as a general obligation of customary international human rights law').

[65] 2021 GGE Report, *supra* note 18, at 13, Norm 13(g); see also *ibid.* at 13 (noting that each state determines 'the structural, technical, organizational, legislative and regulatory measures necessary to protect their critical infrastructure').

[66] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/68/98*, 24 June 2013, para. 19.

to play in this constitutional moment for the international law on cyber operations. Though we are not the lawmakers, scholars contribute to the project of establishing international law for cyberspace both by pointing towards how international law might evolve[67] and by clarifying areas that it does not yet cover, as this article attempts to accomplish. There is much left to do.

[67] Coco, Dias and van Benthem, *supra* note 50.