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

Illegal: The SolarWinds Hack under International Law

Antonio Coco,[*] Talita Dias[**] and Tsvetelina van Benthem[***]

Abstract

In late 2020, news surfaced about one of the most extensive attacks on an information technology (IT) supply chain to date. Hackers exploited a vulnerability in the update system of Orion, a network-monitoring and management software developed by the company SolarWinds. Malicious code embedded in Orion updates created a backdoor into the systems used by numerous private and public entities. This backdoor was then used to insert additional malware into affected systems – in particular, spyware to exfiltrate confidential or sensitive data. Considering both the importance of preserving the integrity of IT supply chains and the diverse risks of harm that attacks such as the SolarWinds hack give rise to, this article examines this cyber operation according to the relevant rules of international law – notably those on sovereignty, non-intervention, general due diligence duties and international human rights law. It concludes that the operation may have been illegal on multiple fronts.

1 Introduction

The so-called 'SolarWinds hack' made the headlines in late 2020 as 'the largest and most sophisticated sort of operation [ever] seen'.[1] The cyber operation exploited a

[*] Lecturer, School of Law, University of Essex, Colchester; Visiting Fellow, Oxford Institute for Ethics, Law and Armed Conflict, Blavatnik School of Government, University of Oxford (Oxford ELAC), United Kingdom. Email: antonio.coco@essex.ac.uk.

[**] Shaw Foundation Junior Research Fellow in Law, Jesus College, University of Oxford; Research Fellow, Oxford ELAC, United Kingdom. Email: talita.desouzadias@bsg.ox.ac.uk.

[***] DPhil Candidate, Faculty of Law, University of Oxford; Lecturer in Public International Law, Department of Continuing Education, University of Oxford; Research Associate, Oxford ELAC, United Kingdom. Email: tsvetelina.vanbenthem@merton.ox.ac.uk.

We would like to thank Dapo Akande, Duncan Hollis and Harold Koh for their helpful comments on earlier drafts. Any error remains, of course, our own.

For an opposing view, see Eichensehr, 'Not Illegal: The SolarWinds Incident and International Law', 33 *European Journal of International Law* (2022) 1263, available at https://doi.org/10.1093/ejil/chac060.

[1] K. Paul, 'SolarWinds Hack Was Work of "At Least 1,000 Engineers", Tech Executives Tell Senate', *The Guardian* (24 February 2021), available at www.theguardian.com/technology/2021/feb/23/solarwinds-hack-senate-hearing-microsoft.

vulnerability in the update system of Orion, a network-monitoring and management software developed by Texas-based company SolarWinds. While, on its face, unremarkable, this programme plays a significant part in the so-called 'information technology' (IT) supply chain of the USA and at least seven other countries: a widespread network of private and public actors using different IT products for the provision of key services, ranging from energy to health and education. Malicious code embedded in Orion updates created a backdoor into the systems used, among others, by cyber-security firm FireEye,[2] Microsoft,[3] Cisco, at least a hospital and a university[4] and a number of US governmental agencies.[5] This backdoor was then used to insert additional malware into affected systems – in particular, spyware to exfiltrate confidential or sensitive data.

While the purpose of the operation may have been primarily espionage, it is now clear that the harm it caused was multi-layered, pervasive and reaching far beyond its targets of interest. In particular, by compromising a software update system used by thousands of users worldwide, the hack has undermined public trust in a fundamental cyber-security mechanism.[6] Even more worrying is what could have happened and what might still happen in similar future operations. For instance, the official announcement that 'Black Start' – the detailed US plans to restore power in the event of a cataclysmic blackout – was compromised during the operation prompted some to speculate that the hackers were hoping to gain backdoor access into the US electric grid and laboratories developing and transporting new generations of nuclear weapons. It cannot be excluded, at this stage, that this and other pieces of malware inserted through this hack or other vulnerabilities[7] may eventually have detrimental effects on operational

[2] FireEye, 'Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims with SUNBURST Backdoor', *Mandiant* (13 December 2020), available at www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html.

[3] 'Microsoft Internal Solorigate Investigation Update', *Microsoft Security Response Center* (31 December 2020), available at https://msrc-blog.microsoft.com/2020/12/31/microsoft-internal-solorigate-investigation-update/.

[4] K. Poulsen, R. McMillan and D. Volz, 'SolarWinds Hack Victims: From Tech Companies to a Hospital and University', *Wall Street Journal* (21 December 2020), available at www.wsj.com/articles/solarwinds-hack-victims-from-tech-companies-to-a-hospital-and-university-11608548402.

[5] D. Sanger, N. Perlroth and J. Barnes, 'As Understanding of Russian Hacking Grows, So Does Alarm', *New York Times* (2 January 2021), available at www.nytimes.com/2021/01/02/us/politics/russian-hacking-government.html.

[6] J. Westby, 'SolarWinds Cyber Attacks Raise Questions About the Company's Security Practices and Liability', *Forbes* (16 December 2020), available at www.forbes.com/sites/jodywestby/2020/12/16/solarwinds-cyber-attacks-raise-questions-about-the-companys-security-practices-and-liability/.

[7] S. Vaughan-Nichols, 'SolarWinds: The More We Learn, the Worse It Looks', *ZDNet* (4 January 2021), available at www.zdnet.com/article/solarwinds-the-more-we-learn-the-worse-it-looks/; C. Cimpanu, 'A Second Hacking Group Has Targeted Solarwinds Systems', *ZDNet* (21 December 2020), available at www.zdnet.com/article/a-second-hacking-group-has-targeted-solarwinds-systems/; Software Engineering Institute, CERT Coordination Center, 'SolarWinds Orion API Authentication Bypass Allows Remote Command Execution', *Carnegie Mellon University* (28 January 2021), available at https://kb.cert.org/vuls/id/843464.

technology[8] – that is, 'programmable systems or devices that interact with the physical environment'.[9]

These considerations highlight the dangers of tampering with IT supply chains.[10] Whilst cyber-security policies and measures are often focused on the protection of the end user's own systems and infrastructure, weak links in the IT supply chain may be more vulnerable and, thus, seen as particularly enticing targets.[11] Compromised products or services supplied through such chains may be used by a wide variety of users – public and private – greatly facilitating the spread of malicious code and widening the pool of possible targets, as was the case for SolarWinds. For this reason, multiple norms of responsible state behaviour in the use of information and communications technologies (ICTs), recommended by the United Nations (UN) Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (GGE), concern the integrity of the IT supply chain.[12]

Considering both the importance of preserving the integrity of IT supply chains and the diverse risks of harm that operations such as the SolarWinds hack may give rise to, in what follows, we assess its legality under international law. The hack was met with a flurry of political statements and academic commentary. With the benefit of temporal distance, now is a good time for a sober legal analysis, starting with five preliminary points. First, as some of us have argued elsewhere,[13] we accept that international law applies in full and by default to ICTs. Second, international law does not protect IT supply chains *per se*. Rather, it regulates specific types of conduct – actions and omissions – that impact the legally protected interests of states, private entities and individuals. Thus, protection under international law depends not on the IT products themselves but, rather, on who uses them and for what purpose. Third, operations such as the SolarWinds hack, which unfold primarily as breaches of confidentiality of

[8] J. Weiss and B. Hunter, 'The SolarWinds Hack Can Directly Affect Control Systems', *Lawfare* (22 January 2021), available at www.lawfareblog.com/solarwinds-hack-can-directly-affect-control-systems.

[9] 'Glossary: Operational Technology', *US National Institute of Standards and Technology*, available at https://csrc.nist.gov/glossary/term/operational_technology.

[10] K. Townsend, 'Huawei and Supply Chain Security: The Great Geopolitical Debate', *SecurityWeek* (27 January 2020), available at www.securityweek.com/huawei-and-supply-chain-security-great-geopolitical-debate; G. Kadiri and J. Tilouine, 'A Addis-Abeba, le siège de l'Union africaine espionné par Pékin', *Le Monde* (26 January 2018), available at www.lemonde.fr/afrique/article/2018/01/26/a-addis-abeba-le-siege-de-l-union-africaine-espionne-par-les-chinois_5247521_3212.html; J. Sherman, 'What's the Deal with Huawei and a Hack at African Union Headquarters?', *Duke University Voices* (31 May 2019), available at https://medium.com/dukeuniversity/whats-the-deal-with-huawei-and-a-hack-at-african-union-headquarters-1e454c1f31a2.

[11] Heinl, 'Recommendation 13(i)', in United Nations (UN) Office for Disarmament Affairs (ed.), *Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology: A Commentary* (2017) 223, at 228, para. 17.

[12] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE Report 2015), UN Doc. A/70/174, 22 July 2015, para. 13(i); see also letters (g) and (j).

[13] Akande, Coco and Dias, 'Drawing the Cyber Baseline: The Applicability of Existing International Law to the Governance of Information and Communication Technologies', 99 *International Law Studies* (2022) 4.

infiltrated systems, bring us directly into a topic that is almost 'taboo' in international legal discourse: espionage. Early legal[14] and policy[15] commentary on SolarWinds focused on its cyber-espionage dimension, overwhelmingly concluding that the operation was politically legitimate and/or lawful under international law. However, it is worth stressing that there is no espionage exception to the application of other rules of international law.[16] This means that, even if there is no prohibition of espionage *per se*, it may very well be that certain espionage operations, through their means, methods or effects, violate applicable international law. Fourth, even if international law is not displaced by the intelligence-gathering purpose of the operation, uncertainty remains in its application in this and similar scenarios involving harmful cyber operations. The relevant rules – sovereignty, non-intervention, human rights, among others – all contain their own interpretative controversies. But even if these questions emerge recurrently,[17] the discussion has evolved and grown in sophistication, reigniting and shedding new light on foundational debates in international law.[18] Fifth, any discussion of the legality under international law of the SolarWinds and similar hacks necessarily begins with the question of attribution of conduct to a state.[19] Attribution of cyber operations is a notoriously difficult question in its own right, but it falls beyond the scope of this article.[20] For the sake of analysis, we assume that the SolarWinds hack is attributable to a state, a conclusion that was drawn by the USA when formally attributing the operation to Russia.[21]

[14] See, e.g., K. Eichensehr, '"Strategic Silence" and State-Sponsored Hacking: The US Gov't and SolarWinds', *JustSecurity* (18 December 2020), available at www.justsecurity.org/73921/strategic-silence-and-state-sponsored-hacking-the-us-govt-and-solarwinds/; A. Lubin, 'SolarWinds as a Constitutive Moment: A New Agenda for the International Law of Intelligence', *JustSecurity* (23 December 2020), available at www.justsecurity.org/73989/solarwinds-as-a-constitutive-moment-a-new-agenda-for-the-international-law-of-intelligence/.

[15] J. Goldsmith, 'Quick Thoughts on the Russia Hack', *Lawfare* (16 December 2020), available at www.lawfareblog.com/quick-thoughts-russia-hack; C. Martin, 'Cyber "Deterrence": A Brexit Analogy', *Lawfare* (15 January 2021), available at www.lawfareblog.com/cyber-deterrence-brexit-analogy.

[16] M. Schmitt (ed.), *Tallinn Manual 2.0* (2nd edn, 2017), at 168, rule 32. *Contra* R. Buchan, 'Eye on the Spy: International Law, Digital Supply Chains and the SolarWinds and Microsoft Hacks', *Völkerrechtsblog* (31 March 2021), available at https://voelkerrechtsblog.org/eye-on-the-spy/.

[17] See, e.g., Milanovic and Schmitt, 'Cyber Attacks and Cyber (Mis)information Operations during a Pandemic', 11 *Journal of National Security Law and Policy* (2020) 247.

[18] See, e.g., 'Basic Position of the Government of Japan on International Law Applicable to Cyber Operations', *Ministry of Foreign Affairs of Japan* (28 May 2021), available at www.mofa.go.jp/policy/page3e_001114.html; and 'International Law and Cyberspace: Finland's National Positions', *Finland Government* (15 October 2020), available at https://um.fi/documents/35732/0/Cyber+and+international+law%3B+Finland%27s+views.pdf/41404cbb-d300-a3b9-92e4-a7d675d5d585?t=1602758856859.

[19] International Law Commission (ILC), Articles on Responsibility of States for Internationally Wrongful Acts, GA Res. 56/83, 12 December 2000, art. 2(a).

[20] Mikanagi and Mačák, 'Attribution of Cyber Operations: An International Law Perspective on the Park Jin Hyok Case', 9 *Cambridge International Law Journal* (2020) 51; Eichensher, 'The Law and Politics of Cyberattack Attribution', 67 *University of California Los Angeles Law Review* (2020) 520.

[21] '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/; K. Eichensehr, 'SolarWinds: Accountability, Attribution, and Advancing the Ball', *JustSecurity* (16 April 2021), available at www.justsecurity.org/75779/solarwinds-accountability-attribution-and-advancing-the-ball/.

In what follows, we analyse two main 'families' of international obligations. On the one hand, we query whether carrying out or supporting the SolarWinds hack constituted a breach of certain international obligations to refrain from causing harm to other states and individuals. Such 'negative' duties may derive from (i) international law protecting state sovereignty; (ii) the principle of non-intervention; and (iii) international human rights law. On the other hand, we inquire whether SolarWinds and similar IT supply chain attacks engage states' positive duties to prevent and redress harm by third parties. These obligations include the *Corfu Channel* and no-harm principles as well as positive human rights obligations, all of which require states to exercise due diligence in their use of ICTs.[22] We conclude that the operation was likely illegal under most of these rules.

2 The SolarWinds Hack as Unlawful Conduct

A *States' Sovereign Rights over Cyber Infrastructure*

If the SolarWinds hack was indeed carried out by a state actor against IT systems used in or by other states, it may qualify as a violation of state sovereignty.[23] Two difficulties ought to be cleared before finding such a violation. First, the very existence of a specific rule protecting state sovereignty is questioned. Second, the scope of such a rule is contested – that is, it is not yet settled which types of unauthorized intrusions into a state's digital infrastructure would constitute a violation.

Assuming that a specific rule protecting state sovereignty exists, a breach may arise by an infringement upon a state's territorial integrity or interference with inherently sovereign functions. Beyond the infliction of physical damage or injury in another state's territory or areas under its effective control, there is controversy as to how a state's territorial integrity may be violated. Specifically, it is unclear whether causing a 'loss of functionality' of cyber infrastructure located in another state suffices for a

[22] The so-called 'Corfu Channel principle' refers to the 'principle of prevention' articulated by the International Court of Justice in the *Corfu Channel* case as 'every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States'. See *Corfu Channel (United Kingdom v. Albania)*, Judgment, 9 April 1949, ICJ Reports (1949) 22.

[23] M. Schmitt, 'Top Expert Backgrounder: Russia's SolarWinds Operation and International Law', *JustSecurity* (21 December 2020), available at www.justsecurity.org/73946/russias-solarwinds-operation-and-international-law/. The rule is supported, for example, by France ('International Law Applied to Operations in Cyberspace', paper shared by France with the Open-ended working group established by Resolution 75/240, *United Nations Office for Disarmament Affairs* [2021], at 2–3, available at https://documents.unoda.org/wp-content/uploads/2021/12/French-position-on-international-law-applied-to-cyberspace.pdf) and Iran (Declaration of General Staff of the Armed Forces of the Islamic Republic of Iran Regarding International Law Applicable to the Cyberspace, July 2020, Art. II, available at www.aldiplomasy.com/en/?p=20901). *Contra, inter alia*, 'Application of International Law to States' Conduct in Cyberspace', *UK Government* 3 June 2021, para. 4, available at www.gov.uk/government/publications/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement; see also *Tallinn Manual 2.0*, *supra* note 16, at 17, rule 4.

breach of sovereignty. The experts involved in the *Tallinn Manual 2.0* agreed that a violation of sovereignty would ensue if the loss of functionality entailed the need to repair or replace physical components of the targeted cyber infrastructure or compromised physical equipment reliant on such infrastructure.[24] Such effects would be akin to physical damage.[25] There is no evidence that the SolarWinds hack produced such results. Nevertheless, as noted earlier, the risk of remote damage or disruption to operational technology controlling physical devices remains latent.

Additionally, some *Tallinn Manual* experts suggested that loss of functionality entailing a violation of sovereignty would occur if 'the operating system or other data[base] upon which the targeted cyber infrastructure relies in order to perform its intended purpose' needs to be reinstalled (not merely rebooted).[26] Reinstallation of affected programmes is exactly what the US Cybersecurity and Infrastructure Security Agency (CISA) directed all affected users to do following the SolarWinds hack.[27] To be sure, Orion, the targeted software, did not stop functioning altogether because of the hack, even if, to remove the infection, affected companies and institutions had to replace programmes and/or rebuild their networks, incurring significant costs. One could nonetheless argue that Orion did stop working as it should – that is, with the necessary safety functions. After all, who would use a network-monitoring software involving sensitive data if there was no safety mechanism to protect it against data breaches? This seems to be a paradigmatic example of the loss of a core software function, meeting the required threshold.

In any event, violations of sovereignty may also arise from remote interference with a state's inherently governmental functions, whether with physical or non-physical manifestations.[28] There is no question that the functions exercised by the US Treasury, State and Energy departments, along with the Pentagon – all significantly affected by the SolarWinds hack – are inherently sovereign. Thus, at the very least, insofar as remote control was obtained over these key governmental IT systems, a violation of US sovereignty occurred.

B *Rule of Non-Intervention*

Whether or not a specific rule protecting sovereignty exists in international law, the SolarWinds hack may have constituted an unlawful act of intervention in the USA's internal affairs. The hack posed a significant threat to US national security. As noted above, it targeted, among many others, the US Treasury and Commerce departments as well as the Energy Department, which is responsible for the management of US nuclear weapons. Ensuring cyber defences appropriate to remediate this breach has been a complex and costly endeavour.[29] A glance at the American Rescue Plan shows

[24] *Tallinn Manual 2.0*, *supra* note 16, at 21.

[25] Schmitt, *supra* note 23.

[26] *Tallinn Manual 2.0*, *supra* note 16, at 21.

[27] 'Emergency Directive 21-01: Mitigate SolarWinds Orion Code Compromise', *US Cybersecurity and Infrastructure Security Agency* (13 December 2020), available at https://cyber.dhs.gov/ed/21-01/.

[28] *Tallinn Manual 2.0*, *supra* note 16, at 21–22.

[29] 'President Biden Announces American Rescue Plan', *White House* (20 January 2021), available at www.whitehouse.gov/briefing-room/legislation/2021/01/20/president-biden-announces-american-rescue-plan/.

that the hack led to a quick rearrangement of priorities at the time of a raging global pandemic.

According to the International Court of Justice (ICJ) in *Nicaragua*, a prohibited intervention bears 'on matters in which each state is permitted, by the principle of state sovereignty, to decide freely'.[30] Examples include 'the choice of a political, economic, social and cultural system, and the formulation of foreign policy' (so-called *domaine réservé*), whether these are carried out by private or public entities.[31] Moreover, a wrongful intervention is one that 'uses methods of coercion in regard to such choices, which must remain free ones'.[32] Following the SolarWinds hack, the breadth of the mitigation measures put forward by CISA,[33] together with the drastic increase in government funds dedicated to cyber-security and modernization projects, signal that policy choices falling within the USA's *domaine réservé* were significantly impacted. When the threatened or actual harm of a cyber operation results in a policy choice that the state would not have made without that operation, there may be a strong indication of an intervention into a state's zone of free choice.

Coercion is precisely about that: depriving a state of its freedom of choice, making it do things it would not otherwise do by means such as force, threats, deception and other non-consensual acts.[34] But it remains unclear whether 'coercion' implies some form of intentionality *vis-à-vis* the result of the operation. Experts disagree on this point.[35] Especially in operations where the primary purpose is espionage, this question becomes critical. In *Nicaragua*, the ICJ did not speak of intention in the paragraphs specifying the content of the non-intervention rule.[36] Thus, if it is not intention but, rather, foreseeability of effects that counts, the SolarWinds hack was illegal under the rule.

3 The Failure to Protect against the SolarWinds Hack as Unlawful Conduct

Irrespective of attribution, the state from whose territory the operation originated may also have violated positive international obligations. As some of us have argued elsewhere,[37] states are bound by several protective international obligations requiring

[30] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States)*, Judgment, 27 June 1986, ICJ Reports (1987) 14.

[31] Schmitt, *supra* note 23.

[32] *Nicaragua*, *supra* note 30, para. 205.

[33] 'Alert (AA20-352A): Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations', *US Cybersecurity and Infrastructure Security Agency* (17 December 2020; updated 15 April 2021), available at https://us-cert.cisa.gov/ncas/alerts/aa20-352a.

[34] S. Wheatley, 'Cyber and Influence Operations Targeting Elections: Back to the Principle of Non-Intervention', *EJIL:Talk!* (26 October 2020), available at www.ejiltalk.org/cyber-and-influence-operations-targeting-elections-back-to-the-principle-of-non-intervention/; *Tallinn Manual 2.0*, *supra* note 16, at 317–318.

[35] *Tallinn Manual 2.0*, *supra* note 16, at 318 (emphasis added).

[36] *Nicaragua*, *supra* note 30, para. 240.

[37] Coco and Dias, '"Cyber Due Diligence": A Patchwork of Protective Obligations in International Law', 32 *European Journal of International Law* (2021) 771.

them to exercise 'due diligence' with a view to preventing, stopping or redressing certain harmful cyber operations. Two of these rules are of general application in international law: the so-called *Corfu Channel* and no-harm principles.

A *The* Corfu Channel *Principle*

In the 1949 *Corfu Channel* case, the ICJ famously held that it is 'every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States'.[38] This duty to protect the rights of other states applies regardless of attribution – that is, who or what was responsible for the harmful conduct. Like other due diligence obligations, compliance with the *Corfu Channel* principle depends on the duty-bearer's actual or constructive knowledge of the act in question and its reasonable capacity to prevent or halt it in the circumstances.[39] As affirmed by the *Tallinn Manual 2.0* experts,[40] the signatories of the Oxford Statements on International Law Protections in Cyberspace[41] and several states,[42] this duty applies by default to states' use of ICTs.

It appears that SolarWinds originated from Russia and has had significant adverse consequences for other states, including the USA and the United Kingdom. We have argued that some of these consequences may have amounted to violations of sovereignty and non-intervention, at the very least with respect to the USA. Irrespective of whether sovereignty is protected by a self-standing rule, and whether interventions are only prohibited if intentionally coercive, the hack was contrary to the victim state's right to carry out its sovereign functions freely.

It is also likely that the hack was contrary to the duty to protect foreign nationals from unfair competition.[43] This obligation is found in Article 10bis of the 1967 Paris Convention for the Protection of Industrial Property,[44] incorporated in Article 2.1 of the World Trade Organization's 1994 Agreement on Trade-Related Aspects of Intellectual Property Rights.[45] Notably, both Russia and the USA are parties thereto. Whether or not industrial espionage is covered by these provisions,[46] the SolarWinds

[38] *Corfu Channel*, *supra* note 22, at 22.

[39] See, e.g., *Tallinn Manual 2.0*, *supra* note 16, at 47; Bannelier-Christakis, 'Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations?', 14 *Baltic Yearbook of International Law* (2014) 23, at 37.

[40] *Tallinn Manual 2.0*, *supra* note 16, at 30, rule 6.

[41] See, e.g., 'The Oxford Statement on International Law Protections in Cyberspace: The Regulation of Ransomware Operations', *Oxford Institute for Ethics, Law and Armed Conflict*, paras 4–5, available at https://elac.web.ox.ac.uk/the-oxford-statement-on-ransomware-operations. Other statements, enshrining similar language, are available at https://elac.web.ox.ac.uk/the-oxford-process.

[42] See, e.g., Basic Position of the Government of Japan', *supra* note 18, at 5; 'International Law Applied to Operations in Cyberspace', *supra* note 23, at 10; *contra*, e.g., 'Application of International Law', *supra* note 23, para. 12.

[43] T. Jančárková and T. Minárik, 'Scenario 09: Economic Cyber Espionage', *Cyber Law Toolkit*, available at https://cyberlaw.ccdcoe.org/wiki/Scenario_09:_Economic_cyber_espionage.

[44] 828 UNTS 305.

[45] 1869 UNTS 299.

[46] R. Buchan, 'Economic Espionage under International Law', *EJIL:Talk!* (16 January 2019), available at www.ejiltalk.org/economic-espionage-under-international-law/.

hack did constitute an act of unfair competition, given its insidiousness, scale and consequences for public and private entities. No fewer than 18,000 institutions were affected, among which were several leading IT companies whose sensitive files on developing technologies may have been accessed and whose reputation may have been permanently tainted.[47] The origin state, insofar as it should have known about the hack and failed to exercise due diligence with a view to preventing or halting it, breached the *Corfu Channel* principle.

B *The No-Harm Principle*

Even if the SolarWinds hack did not result in acts contrary to the rights of other states, the origin state may have violated the so-called no-harm principle. This principle requires states to exercise due diligence in preventing, stopping or redressing foreseeable and significant transboundary harm, including where it results from lawful activity carried out by non-state actors.[48] According to the International Law Commission (ILC), the principle covers 'harm caused to persons, property or the environment', including 'detrimental effects on matters such as, for example, human health, industry, property, environment or agriculture'.[49] Thus, it appears broad enough to cover ICT-related harms.

As the then ILC special rapporteur clarified, the commission's work on the topic concerned 'all physical uses of territory giving rise to adverse physical transboundary effects' and was not limited to 'questions of an ecological nature'.[50] But while the ILC's work was limited to physical consequences for pragmatic reasons of scope,[51] the no-harm principle also applies to non-physical harms. State practice and *opinio juris* in support of this assertion can be found in the ILC's very first survey on the topic,[52] which points to a number of treaties requiring parties to seek to prevent interference with other states' radio broadcasts[53] as well to other treaties extending the duty to any other telecommunications services.[54]

The harm caused by the SolarWinds hack as described above is certainly significant. Assuming that the hack and related harm were foreseeable, and that the origin state

47 Poulsen, McMillan and Volz, *supra* note 4.

48 ILC, Draft Articles on Prevention of Transboundary Harm from Hazardous Activities (Draft Articles), UN Doc. A/56/10 (2001), at 148, para. 1; at 150, para. 6.

49 *Ibid.*, at 152, para. 4.

50 Special Rapporteur Robert Q. Quentin-Baxter, Fourth Report on International Liability for Injurious Consequences Arising Out of Acts Not Prohibited by International Law, UN Doc. A/CN.4/373 and Corr. 1 & 2 (1983), para. 17.

51 Draft Articles, *supra* note 48, at 151, para. 16.

52 ILC, Survey of State Practice Relevant to International Liability for Injurious Consequences Arising Out of Acts Not Prohibited by International Law, UN Doc. A/CN.4/384, 16 October 1984, para. 113.

53 *Ibid.*, paras 58–59 (referring to the International Radiotelegraph Convention 1927, USTS 767; the International Telecommunication Convention 1932, 331 UNTS 1825; and the International Convention Concerning the Use of Broadcasting in the Cause of Peace 1936, 301 UNTS 186).

54 See Constitution and Convention of the International Telecommunication Union 1992, 1825 UNTS 31251, Arts 38(5), 45(3).

failed to exercise due diligence in preventing or mitigating it, such a state is liable to provide reparation for the harm caused. Failing to redress the harm constitutes a violation of the no-harm principle.[55]

4 The SolarWinds Hack as a Violation of Human Rights

International human rights law provides a wide catalogue of duties – both negative and positive – that states are bound to observe online as they do offline. Operations such as the SolarWinds hack can trigger such positive and negative duties under a range of rights, from privacy to life, health and education. Even if the operation was limited to a breach of data confidentiality, the attackers likely accessed not only state secrets but also private information.[56] If personal data, such as employees' credentials, student records or patient information, were accessed, a violation of states' negative and positive obligations to respect and protect the right to privacy under international human rights law may have occurred. While the right to privacy is not absolute, arbitrary interference therewith is prohibited. Such an interference would be arbitrary if it is not prescribed by law, legitimate, necessary or proportionate.[57] Notably, 'any capture of communications data is potentially an interference with privacy and, … the collection and retention of communications data amounts to an interference with privacy whether or not those data are subsequently consulted or used'.[58]

Even mere intrusions into hospital systems and databases can be damaging or at least disruptive to the provision of health care.[59] Whilst the information available on the SolarWinds hack does not allow conclusions to be drawn on this point, concerns arise about the risks that IT supply chain attacks might pose to the rights to life and health. The right to life may be breached when a state does not act to address foreseeable life-threatening harms, regardless of actual loss of life.[60]

That the hack also targeted a university[61] is furthermore cause for concern about a possible interference with the right to education, especially considering that Orion

[55] Draft Articles, *supra* note 48, at 148, para 1; 150, para 6.

[56] Poulsen, McMillan and Volz, *supra* note 4.

[57] Surveillance and Human Rights: Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc. A/HRC/41/35, 28 May 2019, para. 24; The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights, UN Doc. A/HRC/27/37, 30 June 2014, paras 21–30.

[58] Right to Privacy in the Digital Age, *supra* note 57, para. 20.

[59] See, e.g., C. Cimpanu, 'Czech Hospital Hit by Cyberattack While in the Midst of a COVID-19 Outbreak', *ZDNet* (13 March 2020), available at www.zdnet.com/article/czech-hospital-hit-by-cyber-attack-while-in-the-midst-of-a-covid-19-outbreak/; W. Ralston, 'The Untold Story of a Cyberattack, a Hospital and a Dying Woman', *Wired* (11 November 2020), available at www.wired.co.uk/article/ransomware-hospital-death-germany.

[60] Human Rights Committee (HRC), General Comment no. 36 on Article 6 of the International Covenant on Civil and Political Rights, on the Right to Life, Doc. CCPR/C/GC/36, 30 October 2018, paras 6–7.

[61] 'Security Awareness Notice for the University Community', *Kent State University* (2020), available at www.kent.edu/kent/news/security-awareness-notice-university-community.

has been used as a school network management software by several higher education institutions in the USA.[62]

Identifying the state(s) responsible for a breach of negative human rights obligations presupposes tracing the factual origin of the attacks and legally attributing them to one or more states.[63] Conversely, positive human rights duties to protect those rights are owed, and may have been violated, not only by the state(s) harbouring the hackers but also by other states with jurisdiction over individual victims. For both negative and positive human rights obligations, at least under the International Covenant on Civil and Political Rights,[64] jurisdiction may be established extraterritorially to the extent that a state exercises: (i) physical control over the IT communications infrastructure used for the hack; (ii) regulatory control over third parties that control the relevant infrastructure or data;[65] or (iii) functional control over the victims' enjoyment of human rights, even if remote.[66] The functional approach to extraterritorial jurisdiction has not only been endorsed by the UN Human Rights Committee[67] but has also long been advanced by several academics[68] and embraced by at least one state.[69]

Any state with jurisdiction over the individuals affected, including the targeted states, has breached the positive human rights obligations described above insofar as they (i) knew or should have known of the risk of harm arising from the hack; (ii) had the capacity to prevent, mitigate or redress such harm (especially the necessary IT infrastructure and resources); and, yet, (iii) failed to exercise due diligence – that is, their best efforts to protect the rights in question.[70]

5 Conclusion

At a time when the debate about how international law applies to ICTs is fast progressing, the SolarWinds hack has brought to the fore some of the most unsettled aspects of the relevant rules. As we have shown, a strong case can be made that the state to which the hack can be attributed violated its negative duties to respect the sovereignty and not to intervene in the internal affairs of, at least, the USA. It may also be held liable for violating human rights, notably the right to privacy. Irrespective of the

[62] B. Foresman, 'After SolarWinds Attack, Universities Double-check for Compromise', *EdScoop* (29 December 2020), available at https://edscoop.com/after-solarwinds-attack-universities-double-check-for-compromise/.

[63] E.g. 'Fact Sheet', *supra* note 21.

[64] International Covenant on Civil and Political Rights 1966, 999 UNTS 171.

[65] Right to Privacy in the Digital Age, *supra* note 57, paras 31–36.

[66] General Comment no. 36, *supra* note 60, paras 21 and 63.

[67] *Ibid.*

[68] See, e.g., Cleveland, 'Embedded International Law and the Constitution Abroad', 110 *Columbia Law Review* (2010) 225; Shany, 'Taking Universality Seriously: A Functional Approach to Extraterritoriality in International Human Rights Law', 7 *Law and Ethics of Human Rights* (2013) 47.

[69] Germany in Bundesverfassungsgericht (BVerfG), Bundesnachrichtendienst Case, 1 BvR 2835/17, 19 May 2020, available at www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2020/bvg20-037.html.

[70] In more detail, see Coco and Dias, *supra* note 37, at 795–800.

legal attribution of the hack to any particular entity, the hack's origin state appears to have breached the *Corfu Channel* and no-harm principles by failing to exercise due diligence in preventing, halting or redressing the harm resulting from the hack. Any state with jurisdiction over the individuals affected, including the targeted states, may have also breached their positive obligations to protect human rights from the risk of harm. Categorical answers are difficult in this environment where 'operating in the grey' is almost elevated to a virtue. However, what academic commentary and state reactions around the SolarWinds hack have demonstrated is that, when certain types of operations raise the risk of harm beyond tolerable levels, zones of legal certainty ought to be highlighted.