


ORIGINAL ARTICLE

INTERNATIONAL LAW AND PRACTICE

# Legal challenges of attributing malicious cyber activities against space activities

Du Li<sup>\*</sup> 

Law School, Hainan University, Haikou, China  
Email: [li.du@hainanu.edu.cn](mailto:li.du@hainanu.edu.cn)

## Abstract

Malicious cyber activities against space activities (MCASAs) add to the complexities of the legal attribution of malicious cyber activities violating international law. The ‘space’ implies the possibility of applying international space law considering the *lex specialis derogat legi generali* (more specific rules will prevail over more general rules) principle. However, neither the attribution rules of international space law nor of general international law could completely tackle this dilemma. This study categorizes MCASAs into three categories based on the role of the involved space activities and analyses the crux of legal attribution in each scenario. It proposes different coping approaches, including a four-pronged way, introducing a peculiarity test, and specifying substantive international obligations of the states responsible for space activities.

**Keywords:** malicious cyber activities; legal attribution; space activities; state responsibility; the *lex specialis derogat legi generali* principle

## 1. Introduction

With proliferating cyber threats and the occurrence of several malicious cyber activities, the issue of legal attribution for establishing the states’ responsibility challenges the prevailing attribution rules and raises extensive scholarly discussions. Without a concrete and widely recognized solution to the cyber attribution problem, the advent of malicious cyber activities against space activities (MCASAs) complicates the existing dilemma. The added ‘space’ factor introduces the possibility of applying international space law for coping with the attribution issues according to the maxim *lex specialis derogat legi generali* (more specific rules will prevail over more general rules), as crystallized in Article 55 of the International Law Commission (ILC) Articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA).<sup>1</sup>

The imminency of the threats posed by MCASAs prompts the necessity to address relevant legal challenges. In 1998, a critical optical sensor of the German-United States (US) ROSAT space telescope was damaged following a cyber-intrusion at the Goddard Space Flight Centre.<sup>2</sup> Several incidents have been reported in 2007 and 2008, such as the cyber interference suffered by Landsat

<sup>\*</sup>The author sincerely appreciates the insightful and constructive comments and recommendations from the anonymous reviewers. This work was financially supported by the Education Department of Hainan Province [grant number Hnky2023ZD-1] and Hainan University [grant number kyqd(sk)2101].

<sup>1</sup>ILC Articles on Responsibility of States for Internationally Wrongful Acts, 2001 YILC, Vol. II (Part Two).

<sup>2</sup>W. Akoto, ‘Hackers Could Shut Down Satellites – or Turn Them into Weapons’, *The Conversation*, 12 February 2020, available at [theconversation.com/maliciousactors-could-shut-down-satellites-or-turn-them-into-weapons-130932](https://theconversation.com/maliciousactors-could-shut-down-satellites-or-turn-them-into-weapons-130932).

7 in 2007 and 2008, and by Terra (EOS AM-1) in 2007,<sup>3</sup> and the hijacking of Intelsat-12 satellite by Liberation Tigers of Tamil Eelam in 2007.<sup>4</sup> GPS hackings have been reported from time to time.<sup>5</sup> The ViaSat incident of 2022 is a more recent illustration. Exacerbating this situation, space assets and systems are vulnerable to malicious cyber activities<sup>6</sup> and are becoming increasingly connected and interoperable, whether governmental, commercial, national, or multinational.<sup>7</sup> The growing cases of MCASAs and their potential consequences testify to the necessity of tackling the issue, which could be evidenced by the initiatives taken at the international and national levels. The 'Space 2030' agenda and the global governance of outer space activities adopted by the United Nations (UN) Committee on the Peaceful Uses of Outer Space (COPUOS) in 2018 proposed the consideration of critical space infrastructure at the international level, including a study of cyber-security issues related to space activities.<sup>8</sup> The Ukrainian delegation, in 2021, proposed including the cyber-security of space activities on the agenda of the UN COPUOS Legal Subcommittee.<sup>9</sup> National practices to enhance the cyber-security of space activities and combat MCASAs are emerging.<sup>10</sup> Identifying states' responsibility and holding states accountable when they fail in their duties are vital legal means to cope with this issue.

To combat MCASAs, it is crucial to address their attribution dilemma. International space law confers outer space a peculiar legal status, founded typically by Article II of the Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies (Outer Space Treaty [OST]).<sup>11</sup> It stipulates that 'outer space, including the Moon and other celestial bodies, is not subject to national appropriation by claim of sovereignty, by means of use of occupation, or by any other means'. Per this article, it is commonly agreed that no state parties would be entitled to exercise territorial jurisdiction over any part of outer space or celestial bodies. Moreover, outer space, including the Moon and other celestial bodies, constitutes an area beyond national jurisdiction.<sup>12</sup> The legal status of outer space distinguishes it from other areas on Earth, except for the high seas, the seabed beyond the limits of the continental shelf, and polar areas. Nonetheless, this does not imply that outer space is an area without order or responsibility. Instead, the limited scope of application of international space law endows it with the status of *lex specialis* (special law).<sup>13</sup> International space law provides for states' international obligations in the conduct of space activities. According to Article 2 of the ARSIWA, attribution and the breaching of international obligations are vital elements for an act or omission to constitute an internationally wrongful act. Several branches of international law are applicable

<sup>3</sup>J. Muylaert and L. Del Monte, 'Cybersecurity of Space Missions', Presentation at the Workshop of the European Interparliamentary Space Conference of 14 May 2018.

<sup>4</sup>Intelsat, 'Intelsat Works with Sri Lankan Authorities to Halt Unauthorized Use of Its Satellite', 11 April 2007, available at [investors.intelsat.com/news-releases/news-release-details/intelsat-works-sri-lankan-authorities-halt-unauthorized-use-its](https://investors.intelsat.com/news-releases/news-release-details/intelsat-works-sri-lankan-authorities-halt-unauthorized-use-its).

<sup>5</sup>P. Tullis, 'GPS Is Easy to Hack, and the U.S Has No Backup', *Scientific American*, 1 December 2019, available at [www.scientificamerican.com/article/gps-is-easy-to-hack-and-the-u-s-has-no-backup/](https://www.scientificamerican.com/article/gps-is-easy-to-hack-and-the-u-s-has-no-backup/).

<sup>6</sup>R. von Solms and J. van Niekerk, 'From Information Security to Cyber Security', (2013) 38 *Computers and Security* 97.

<sup>7</sup>D. Li, 'Cyber-Attacks on Space Activities: Revisiting the Responsibility Regime of Article VI of the Outer Space Treaty', (2023) 63 *Space Policy* 101522, at 1.

<sup>8</sup>UNGA, The 'Space2030' Agenda and the Global Governance of Outer Space Activities, UN Doc. A/AC.105/1166 (13 December 2017).

<sup>9</sup>Committee on the Peaceful Uses of Outer Space, The Proposal of the Ukrainian Delegation on the Establishment of a New Item on the Agenda of the Legal Subcommittee on the Cybersecurity of Space Activities, UN Doc. A/AC.105/C.2/2021/CRP.27 (8 June 2021).

<sup>10</sup>See, for instance, White House, National Security & Defense: Memorandum on Cybersecurity Principles for Space Systems, 4 September 2020, Space Policy Directive-5, available at [trumpwhitehouse.archives.gov/presidential-actions/memorandum-space-policy-directive-5-cybersecurity-principles-space-systems/](https://trumpwhitehouse.archives.gov/presidential-actions/memorandum-space-policy-directive-5-cybersecurity-principles-space-systems/).

<sup>11</sup>UNOOSA, Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, UN Doc. A/RES/2222 (XXI) (1967).

<sup>12</sup>B. Cheng, *Studies in International Space Law* (1997), 230; S. Hobe, B. Schmidt-Tedd and K. U. Schrogl (eds.), *Cologne Commentary on Space Law-vol. I* (2009), 48.

<sup>13</sup>H. Thirlway, *The Sources of International Law* (2019), 147.

for demarcating states' international obligations in MCASAs, such as cyber law, *jus ad bellum* (the conditions under which states may resort to war or the use of armed force in general), and international space law. The scope and the exact content of the obligations remain to be determined. However, states' international obligations for certain malicious cyber activities could be addressed through international telecommunications law<sup>14</sup> and by interpreting the current rules. The attribution issue is more challenging. As international space law offers a unique set of attribution rules, departing from the ARSIWA, applying both sets of attribution rules is possible in MCASAs. However, deciding the rule to apply and interpreting the applicable rule are requisite.

This study aims to assess the appropriateness of current attribution rules in determining the responsible state, identify its challenges, and propose solutions to the conundrums. The present study takes a scenario analysis method and proceeds as follows. Section 2 defines the key notions relevant to MCASAs and divides the cases into three scenarios. Sections 3 to 5 analyse the specific attribution problems in each scenario and put forward targeted suggestions to tackle them. Section 6 summarizes and concludes the study.

## 2. Scenarios of MCASAs

Before discussing the different scenarios of MCASAs, the definitions of relevant key notions must be addressed. Cyberspace can be defined as a 'globally accessible technological infrastructure of interconnected computers and networks, which is used for the transmission of signals and data', and cyber activities are based on 'the exchange of digitized data and take place through the use of cyberspace infrastructure using the universal language of code'.<sup>15</sup> Different terms, such as hacking, unauthorized cyber activity, and non-lawful cyber activity, are used as alternatives for malicious cyber activity. Among these, cyberattack is the most common term, which is the process of intruding into computer systems, referring to a type of computer operation that seeks to disrupt, deny, degrade, or destroy information, computers, or computer networks.<sup>16</sup> However, legal professionals avoid using 'cyberattack' broadly because of the different meanings of attack in the law of armed conflict and to avoid defining cyber intrusion as a new means of war.<sup>17</sup> Hence, this study adopts the direct and general term, 'malicious cyber activities against space activities' to refer to cyber intrusions into space systems, enabling the intruder to exploit satellite information without authorization, disrupt the transmission of information by degrading or modifying it, partially damage or destroy a satellite's computer software and hardware, and manipulate the command and control of a satellite, possibly causing collisions, explosions, atmospheric re-entry, depletion of limited resources, or third party damage.<sup>18</sup>

A preliminary problem to consider regarding legally attributing MCASAs is deciding the applicable law, which shall be determined by the nature of the activities. As highlighted by Kaiser, space law applies to cyber activities when they are space activities; thus, defining the application scope of international space law is essential.<sup>19</sup> International space law applies to space-related activities and activities in or concerning outer space,<sup>20</sup> with four major purposes – space

<sup>14</sup>S. Aoki, 'Identifying the Scope of the Applicable International Law Rules towards Malicious Cyber Activities against Space Assets', (2018) 61 *Proceedings of the International Institute of Space Law* 687, at 699.

<sup>15</sup>R. Popova, 'Cyber Law and Outer Space (Activities): Legal and Regulatory Challenges', (2018) 61 *Proceedings of the International Institute of Space Law* 659, at 660.

<sup>16</sup>M. Maybaum, 'Technical Methods, Techniques, Tools and Effects of Cyber Operations', in K. Ziolkowski (ed.), *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy* (2013), 103.

<sup>17</sup>S. A. Kaiser, 'When Cyber Activities Are Space Activities: Definitions Are Key', (2020) 63 *Proceedings of the International Institute of Space Law* 297, at 303.

<sup>18</sup>M. Mejía-Kaiser, 'Space Law and Unauthorised Cyber Activities', in Ziolkowski, *supra* note 16, at 349.

<sup>19</sup>See Kaiser, *supra* note 17, at 297.

<sup>20</sup>F. G. von der Dunk, 'International Space Law', in F. G. von der Dunk and F. Tronchetti (eds.), *Handbook of Space Law* (2015), 29.

exploration, space technology development, space applications, and the implementation of the space exploration and technology results.<sup>21</sup> Malicious cyber activities conducted on Earth against the terrestrial part of a space system may severely impact space activities. However, they do not qualify as space activities as they are neither activities in outer space or of an inherent relation with outer space, nor carried out for any of the four aforementioned purposes. Hence, the first scenario is as follows:

*Scenario one: Malicious cyber activities against terrestrial systems.*

The legal attribution of these malicious conducts should be determined according to general international law. MCASAs that are likely to be identified as space activities can be divided into two categories. First, the orders of the malicious cyber actors may be transmitted through satellites to other space objects or terrestrial receiving stations; or the orders could be directly given to space objects to deorbit and dash into another object. Hence, the second scenario is as follows:

*Scenario two: Malicious cyber activities manipulating space activities.*

Second, with the increasing presence of human beings in outer space, conducting malicious cyber activities in outer space becomes possible. These acts are activities ‘in’ outer space. Under the pretence of exploring outer space, these activities are carried out during space activities, even if the purpose of the malicious cyber activities is not one of the four above-mentioned purposes. Nonetheless, considering the legal status of outer space, applying space law would be a preference. Hence, the third scenario is as follows:

*Scenario three: Malicious activities from outer space.*

### 3. Scenario one: Malicious cyber activities against terrestrial systems

No substantial differences exist between malicious cyber activities against terrestrial systems and conventional malicious cyber activities as they are both terrestrial activities. Hence, the attribution rules of general international law shall apply. However, the general conundrums of cyber attribution persist.

In the context of malicious cyber activities, attribution can be divided into technical and legal attribution.<sup>22</sup> Technical attribution is a question of fact, which is vital to the evidence standard.<sup>23</sup> Tracing the originators of malicious cyber activities is extremely difficult.<sup>24</sup> Several factors contribute to this plight, including the obsolescence of the current foundation of network communications in cyberspace, system vulnerabilities, and the difficulties of modernizing the cyberinfrastructure.<sup>25</sup> Furthermore, the myriad stages of a malicious cyber activity cycle, including the preparatory stage of target identification, reconnaissance, and weaponization, the engagement of the present stage of delivery, exploitation, installation, and actions on the objective, and the

<sup>21</sup>T. Neger and E. Walter, ‘Space Law-An Independent Branch of the Legal System’, in C. Brünner and A. Soucek (eds.), *Outer Space in Society, Politics and Law* (2011), 234, at 238.

<sup>22</sup>Z. Huang, ‘Attribution Rules in ILC’s Articles on State Responsibility: A Preliminary Assessment on Their Application to Cyber Operations’, (2014) 14 *Baltic Yearbook of International Law* 41, at 43.

<sup>23</sup>R. Geiss and H. C. Lahmann, ‘Freedom and Security in Cyberspace: Shifting the Focus Away from Military Responses Towards Non-Forcible Countermeasures and Collective Threat-Prevention’, in Ziolkowski, *supra* note 16, at 623.

<sup>24</sup>H-G. Dederer and T. Singer, ‘Adverse Cyber Operations: Causality, Attribution, Evidence, and Due Diligence’, (2019) 95 *International Law Studies* 430, at 438.

<sup>25</sup>S. J. Shackelford and R. B. Andres, ‘State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem’, (2011) 42 *Georgetown Journal of International Law* 971, at 982.

effects and consequences stage,<sup>26</sup> adds to the difficulties. Currently, technical attribution is possible based on categories of technical indicators. However, errors occur, methodological questions remain open, and the level of confidence in the evidence varies.<sup>27</sup> Although some scholars are optimistic that the technical attribution challenge will be overcome with technological improvements,<sup>28</sup> most scholars hold a pessimistic view.<sup>29</sup>

To the extent that a malicious cyber activity could be technically attributable to an entity, legal attribution issues arise. Although global soft law instruments and regional treaties on cyberspace are mushrooming, there are no universally accepted rules. In addition, the existing norms in cyberspace seldom embrace attribution issues. Applying attribution rules of general international law to malicious cyber activities is inescapable. The legal attribution is straightforward and uncontested when the entity conducting the malicious activity is an organ of a state. The malicious conduct is attributable to the state under Article 4 of the ARSIWA. However, since malicious cyber activities initiated by state organs are seldom reported or admitted, and, in most cases, the malicious actors are individuals or private groups,<sup>30</sup> Article 8 of the ARSIWA is particularly relevant.<sup>31</sup> This article stipulates:

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

Hence, to hold the state accountable, a link between a private malicious actor and the state must be established by evaluating the ‘instruction’, ‘direction’, or ‘control’ exercised by the state over the actor. Some scholars perceive these three words to be different; however, in practice, most commentators blur their distinctions and concentrate on interpreting the single word, ‘control’.<sup>32</sup>

Considering the relevant international jurisprudence, the level of ‘control’ required for attributing an act of private actors to a state is unclear. The issue was addressed in the 1986 *Nicaragua v. United States* case, where the International Court of Justice (ICJ) established the ‘effective control’ standard.<sup>33</sup> Based on the court’s reasoning, to hold a state responsible, it had to be shown that the state possesses effective control over the alleged violations.<sup>34</sup> This standard was reaffirmed in the 2007 *Bosnian Genocide* case in which the ICJ held that the acts of genocide were not attributable to Serbia owing to the lack of effective control over the operations during which the acts took place.<sup>35</sup> In the cyber context, this approach has been deemed inappropriate since it has set an extremely high bar for proof, especially considering the technical attribution

<sup>26</sup>N. Tsagourias and M. Farrell, ‘Cyber Attribution: Technical and Legal Approaches and Challenges’, (2020) 31 EJIL 941, at 946.

<sup>27</sup>*Ibid.*, at 950.

<sup>28</sup>See Y. Dinstein, ‘Computer Network Attacks and Self-Defence’, (2002) 76 *Computer Network Attack and International Law* 99, at 112; M. Roscini, ‘World Wide Warfare - Jus ad Bellum and the Use of Cyber Force’, (2010) 14 *Max Planck Yearbook of United Nations Law* 85, at 97; D. Tran, ‘The Law of Attribution: Rules for Attribution the Source of a Cyber-Attack’, (2018) 20 *Yale Journal of Law & Technology* 376, at 381.

<sup>29</sup>See D. E. Graham, ‘Cyber Threats and the Law of War’, (2010) 4 *Journal of National Security Law & Policy* 87, at 92; M. C. Waxman, ‘Cyber Attacks as “Force” Under UN Charter Article 2(4)’, (2011) 87 *International Law Studies* 43, at 50.

<sup>30</sup>See Huang, *supra* note 22, at 50.

<sup>31</sup>M. N. Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (2013), at 32.

<sup>32</sup>K. Macak, ‘Decoding Article 8 of the International Law Commission’s Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors’, (2016) 21 *Journal of Conflict and Security Law* 405, at 411.

<sup>33</sup>*Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, Merits, Judgment of 27 June 1986, [1986] ICJ Rep. 14, at 54, para. 115.

<sup>34</sup>J. Crawford, *State Responsibility: The General Part* (2013), at 149.

<sup>35</sup>*Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*, Merits, Judgment of 26 February 2007, [2007] ICJ Rep. 43, at 214, para. 413.

difficulties.<sup>36</sup> A less stringent standard, the ‘overall control’ test, was established by the International Criminal Tribunal for the Former Yugoslavia (ICTY) in the *Tadić* case. The Appeals Chamber claimed that in the case of an ‘organised and hierarchically structured group’, overall control would suffice to establish an imputable link.<sup>37</sup> The ICTY noted that overall control must be more than the ‘mere financing and equipping of such forces’ and should entail ‘coordinating or helping in the general planning of military activity’.<sup>38</sup> Although simpler than the effective control standard, this test, too, is quite demanding.<sup>39</sup> The appropriateness of applying the overall control standard in the cyber context is contested since the malicious actors who are, in most cases, individuals or groups of persons loosely organized, may not exhibit the requisite level of organization.<sup>40</sup> Moreover, the effective control and overall control tests do not amount to independent alternatives to the requisite control standard since they apply under different circumstances and fall under varied branches of international law.<sup>41</sup> Although both standards have their supporters,<sup>42</sup> neither fits cyberspace due to their inherent limitations and high-proof requirements.

Apart from judicial precedents, academia has contributed to solving the attribution problems. Some scholars suggest adopting a lower attribution standard, such as applying the idea of imputed responsibility,<sup>43</sup> especially from the perspective of lowering the burden of proof. This method is victim-friendly; however, it needs to be improved in that it would set an extremely high practice standard for the states.<sup>44</sup> It is suggested that cyber-attribution issues should be resolved through co-operation and collaboration between states; however, no substantive routes have been provided.<sup>45</sup> Following this, some scholars proposed introducing a unique legal mechanism, which envisions establishing different institutions.<sup>46</sup>

Setting up a unique standard of attribution is justifiable. As indicated above, the existing attribution standards undermine either the interests of the victim state by imposing an excessive burden of proof or by setting up an impractically high standard of practice. To strike a balance between the victim and the accused, it would be necessary to introduce an alternative attribution standard, which should be set between the effective control and imputed responsibility standards. The ‘virtual control test’ proposed by Margulies<sup>47</sup> seems promising. The test entails a shift of the burden of proof from the victim state to the accused state when the latter funds and equips or knowingly provides sanctuary to a private entity or persons that engage in malicious cyber activities.<sup>48</sup> This serves as a plausible approach for achieving the outcome anticipated by

<sup>36</sup>See Shackelford and Andres, *supra* note 25, at 988; C. Payne and L. Finlay, ‘Addressing Obstacles to Cyber-Attribution: A Model Based on State Response to Cyber-Attack’, (2017) 49 *George Washington International Law Review* 535, at 557; see Macak, *supra* note 32, at 421.

<sup>37</sup>ICTY, *Prosecutor v. Tadić*, Judgement, Case No. IT-94-I-A, Appeals Chamber, 15 July 1999.

<sup>38</sup>*Ibid.*

<sup>39</sup>See P. Margulies, ‘Sovereignty and Cyber Attacks: Technology’s Challenge to the Law of State Responsibility’, (2013) 14 *Melbourne Journal of International Law* 496, at 507; L. Finlay and C. Payne, ‘The Attribution Problem and Cyber Armed Attacks’, (2019) 113 *American Journal of International Law Unbound* 202, at 205.

<sup>40</sup>See Tzagourias and Farrell, *supra* note 26, at 964.

<sup>41</sup>See Macak, *supra* note 32, at 422.

<sup>42</sup>See Shackelford and Andres, *supra* note 25; Huang, *supra* note 22; Finlay and Payne, *supra* note 39.

<sup>43</sup>See Graham, *supra* note 29, at 93; M. J. Sklerov, ‘Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty to Prevent’, (2009) 201 *Military Law Review* 1, at 48.

<sup>44</sup>See Payne and Finlay, *supra* note 36, at 565; Huang, *supra* note 22, at 51–3.

<sup>45</sup>L. Grosswald, ‘Cyberattack Attribution Matters Under Article 51 of the U.N. Charter’, (2011) 36 *Brooklyn Journal of International Law* 1151, at 1155.

<sup>46</sup>See Tzagourias and Farrell, *supra* note 26, at 17–23; Tran, *supra* note 28, at 426–35; Y. Shany and M. N. Schmitt, ‘An International Attribution Mechanism for Hostile Cyber Operations’, (2020) 96 *International Law Studies* 196, at 215–18; W. Banks, ‘Cyber Attribution and State Responsibility’, (2021) 97 *International Law Studies* 1039, at 1070.

<sup>47</sup>See Margulies, *supra* note 39, at 500–1.

<sup>48</sup>*Ibid.*, at 514.



Grosswald, that is, settling the attribution dilemma through co-operation and collaboration between the states since the test can only be realized through international co-operation.

Nonetheless, the virtual control test is not appropriate in all cases, especially when the victim states take retaliatory actions. Margulies proposes that if the information provided by the state virtually controlling another reveals its responsibility or the state refuses to provide the demanded information, the victim state may pursue other remedies, including self-defence.<sup>49</sup> However, the probability of a prolonged back-and-forth process would hinder the victim state from reacting promptly to minimize losses. Scholars have underlined the necessity to apply a high attribution standard when the targeted states take retaliatory actions in the context of malicious cyber activities, such as the 'effective control',<sup>50</sup> as applying a lower standard would lead to conflicts and escalation. Thus, it would be necessary to differentiate circumstances based on the purpose of attributing a malicious cyber activity to a state. The virtual control test is applicable in most cases when the victim state tries to hold a state internationally responsible. Simultaneously, more strict attribution standards should be used when the victim state seeks to respond to such activities.

A specific institution or mechanism for cyber attribution could enhance credibility and complement existing attribution mechanisms,<sup>51</sup> where states and international judiciary authorities play a central role. However, its inherent shortcomings would undermine the accountability of the conclusion. It is reasonable to anticipate a diversification of members' nationalities. Although they may be selected based on their professional qualifications, the internationalization of the membership is likely to render the mechanism a political aspect. The willingness of the states to submit evidence and related information to the institution may be insufficient due to probable information confidentiality. When the state accused of malicious cyber activity is not a member of the specific institution, it would be unlikely for the state to leave the attribution issue to an alien mechanism. The intervention of a specific institution could be time-consuming. Notably, the victim states might take imminent retaliatory actions to avoid further losses. Furthermore, with a well-settled and reasonable attribution standard, judiciary authorities or the victim state could decide independently whether to attribute a particular malicious cyber activity to a certain state without the need for specific institutions.

To sum up, no essential differences exist between malicious cyber activities against terrestrial systems and terrestrial malicious cyber activities regarding technical and legal attribution. The crux of legal attribution lies in establishing the eligible link between private and individual malicious actors and states, igniting the dilemma of determining the 'control' standard. The 'virtual control' test is the most promising among the several standards and approaches proposed by judicial precedents and academia. It is appropriate when the victim state tries to hold a state internationally responsible; however, stricter attribution standards, such as the 'effective control' standard, should be introduced when the victim state seeks retaliatory actions.

In addition, malicious cyber activities against terrestrial systems have been recorded. On 24 February 2022, a multifaceted and deliberate cyberattack against Viasat's KA-SAT network partially interrupted KA-SAT's consumer-oriented satellite broadband service, impacting several thousands of customers in Ukraine and tens of thousands of fixed broadband customers across Europe.<sup>52</sup> After the first technical attribution, the European Union (EU), the US, the United Kingdom (UK), Australia, New Zealand, and Canada released public statements attributing the incident to Russian military intelligence, which were supported by national statements of several

<sup>49</sup>*Ibid.*

<sup>50</sup>See, for example, Dederer and Singer, *supra* note 24, at 446–8; Payne and Finlay, *supra* note 36, at 566; N. Tsagourias, 'Cyber Attacks, Self-Defence and the Problem of Attribution', (2012) 17 *Journal of Conflict and Security Law* 229, at 243–4.

<sup>51</sup>See Shany and Schmitt, *supra* note 46, at 215.

<sup>52</sup>'KA-SAT Network Cyber Attack Overview', *Viasat*, 30 March 2022, available at [news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview](https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview).

states.<sup>53</sup> While the consistent response by these governments contributes to the development of states' practice in political attribution of malicious cyber activities, its significance for solving the dilemma of legal attribution is limited, as the alleged Russian military intelligence is evidently Russia's state organ.

#### 4. Scenario two: Malicious cyber activities manipulating space activities

In malicious cyber activities manipulating space activities, the attribution of malicious actors' conduct may follow the attribution rules of general international law as they do not differ from malicious cyber activities against terrestrial systems from a legal perspective; the complexities and difficulties in both technical and legal attribution are identical. The peculiar predicament of legal attribution lies in applying attribution rules to states whose space activities are manipulated by malicious actors. Since malicious cyber activities manipulating space activities generally involve two or more states, the attribution rules for joint and collective conduct by states must apply.

Joint and collective conduct could be further divided into two categories: (i) where responsibility arises because the state is implicated in the internationally wrongful act of another, whether through the provision of aid or assistance, or by its exercise of control or coercion over the acting state; and (ii) where there is a plurality of responsible states, each of which has breached its international obligations, whether together or separately.<sup>54</sup> Malicious cyber activities manipulating space activities may include both categories; however, the challenges in applying attribution rules differ.

##### 4.1 *Attributing to the states implicated in malicious cyber activities*

A state responsible for a space activity can get implicated in malicious cyber activities initiated by others, whether the latter are states, private entities, or individuals. For instance, the state responsible for the activities in outer space deliberately leaves the malicious actor outside its territory to access the cyber control system of its space systems and issue commands, ordering satellites to transmit commands or deorbit and hit other space objects. Under such circumstances, whether the malicious cyber activity is attributable to the state in which the malicious actor is situated shall be determined according to the attribution rule of general international law. However, attributing the malicious cyber activity to the state conducting the space activities manipulated by the malicious actors shall undergo a double test through primary and secondary rules. Two requirements must be met for establishing the state's responsibility – the state's contribution made through space activities to the joint action is attributable to it, and the contribution amounts to an element of the unlawful act.<sup>55</sup>

In terms of attribution, it is important to decide the applicable rules. Article VI of the OST uses the term 'national activities in outer space' rather than 'national space activities'. If a state party's activities of operating the space systems or leading space missions are considered as activities 'in' outer space, Article VI of the OST shall apply, and these activities are attributable to the state. In contrast, if these activities are deemed unqualified, the attribution rules of general international law apply, leading to a different conclusion. The present dilemma lies in determining the nature of the manipulated activities. There is a division of opinions towards interpreting the term 'national activities in outer space'. Some opine that an activity in outer space is any activity that makes outer space accessible, explorable, or usable. In contrast, others are of the view that it includes an activity that occurs on Earth if it is predominantly and

<sup>53</sup>CyberPeace Institute, 'Viasat Case Study', June 2022, available at [cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat](https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat).

<sup>54</sup>See Crawford, *supra* note 34, at 333.

<sup>55</sup>*Ibid.*, at 335.



intentionally directed at outer space.<sup>56</sup> Kaiser delves into the specific question of when cyber activities are space activities and considers that only when a cyber activity forms an integral part of a space activity can it be qualified as a space activity.<sup>57</sup> The scholarly views, although implying the possibility of treating some activities conducted on Earth as ‘activities in outer space’, however, are inappropriate for deciding the applicable attribution rules in the current circumstances.

Instead, a peculiarity test should be introduced. In some malicious cyber activities manipulating space activities, the impact of the ‘space’ factor on the incident is so trivial that even without the involvement of space activities, the malicious cyber activities could be conducted with successful results. For instance, a malicious actor may intrude into a space system to send orders through communication satellites. This kind of intrusion may be realized through terrestrial networks alone. Whether the orders are sent through space or terrestrial infrastructure has no impact on the malicious activity, and the ‘space’ factor does not demonstrate any peculiarity for achieving the purposes of the malicious actors. Applying the attribution rules of general international law would be more appropriate in such a scenario.

In contrast, when the ‘space’ factor significantly impacts the process or the aftermath of malicious cyber activities, the characteristics of the latter are more ‘spatial’ than ‘terrestrial’, and attribution rules of international space law should apply. For instance, when the purpose of a malicious cyber activity manipulating space activities is to destroy a satellite by intruding into the control system of another satellite and ordering the latter to deorbit and hit the former, the crucial steps of the malicious operation are realized in outer space rather than on Earth. The whole incident would be considered space activity from the perspective of choosing applicable attribution rules.

#### 4.1.1 *Attributing through international space law*

Once the malicious cyber activities manipulating space activities are considered activities in outer space, per the *lex specialis derogat legi generali* principle, the attribution rules of international space law shall apply. However, as highlighted in the commentaries to the ARSIWA, ‘for the *lex specialis* principle to apply . . . there must be some actual inconsistency between them, or else a discernible intention that one provision is to exclude the other’;<sup>58</sup> therefore, the application of the attribution rules of general international law is not completely precluded. International space law is endowed with a different set of attribution rules than the general international law, which is provided in Article VI of the OST:

State parties to the Treaty shall bear international responsibility for national activities in outer space . . . whether such activities are carried on by governmental agencies or by non-governmental entities, and for assuring that national activities are carried out in conformity with the provisions outlined in the present Treaty.

Accordingly, ‘national activities in outer space’ are directly attributable to the state parties, and the crux of establishing the imputable link rests with interpreting the term ‘national activities’.

Several approaches were proposed for identifying national activities, including qualifying the state on whose registry the space object is carried (the state of registry),<sup>59</sup> through the nationality of the individuals participating in the space activities<sup>60</sup> and by determining the states who would

<sup>56</sup>See Hobe, Schmidt-Tedd and Schrogl, *supra* note 12, at 107.

<sup>57</sup>See Kaiser, *supra* note 17, at 303.

<sup>58</sup>*Commentaries to the Draft Articles on Responsibility of States for Internationally Wrongful Acts (2001)*, Report of the ILC, Supplement No. 10 (A/56/10), Ch. IV.E.2.

<sup>59</sup>See Hobe, Schmidt-Tedd and Schrogl, *supra* note 12, at 112.

<sup>60</sup>See 1986 Outer Space Act of the United Kingdom, c. 38 § 1–2.

exercise jurisdiction.<sup>61</sup> The deficiency of the first approach is apparent. While the state of registry may not exercise any actual control over the space object it registered, holding this state internationally responsible for the space activity, although favourable for the victim, would compromise the interests of the state of registry and constitute a loophole favouring the real actor responsible. Identifying national activities according to the nationality of the involved individuals is based on Article IX of the OST, which reads ‘activity or experiment planned by it or its nationals in outer space’ or the international principle of personal jurisdiction.<sup>62</sup> This interpretation is not without shortcomings and cannot be relied upon alone.<sup>63</sup> If this approach were adopted, more than one state would be held directly responsible, including the state of nationality of the space tourism company and the state of nationality of the space tourist who carries out the malicious cyber activity, leading to a chaotic situation where several states could claim unawareness of their nationals’ specific activities. This is true in commercial space activities where individuals and entities from different states may participate in the same space activities. A logical corollary of this application would be extremely stringent restrictions imposed on all space activities by states to avoid state responsibility, leading to stagnation of the space economy. The current international space law does not envision such circumstances and cannot provide any guidance on solving the problem. Bin Cheng supported the third way of interpretation, highlighting that the implied intention under Article VI of the OST is that ‘every State Party should be directly responsible for any space activity that is within its legal power or competence to control’, concluding that any space activity carried on by an entity ‘that is within a State’s jurisdiction . . . qualifies as that state’s “national activity”’.<sup>64</sup> He further underlined that a spacecraft’s state of registry exercises quasi-territorial jurisdiction over the space activities therefrom or on board and recognized personal jurisdiction of a state over its nationals.<sup>65</sup> In the case of competing jurisdiction, it is considered that quasi-territorial jurisdiction prevails over personal jurisdiction,<sup>66</sup> implying that only one state should be held responsible. This interpretation is supported by almost all state practices.<sup>67</sup> In addition to the inconsistency in terminological interpretations, the attribution rules of international space law put the state carrying out the space activity in a central position for international responsibility and do not reflect the inherent relationship between the manipulated space activity and the malicious cyber activity. This is not always reasonable as, in most cases, the state plays a minor role in the whole incident. Hence, an apparent loophole exists in international space law.

#### 4.1.2 *Attributing through general international law*

Applying the attribution rules of general international law to space activities is well-founded. The actual inconsistency between the *lex specialis* and general international law is required for the *lex specialis* principle to apply.<sup>68</sup> No rules in international space law indicate envisaging joint or collective conduct, allowing relevant general international law rules to apply. Albeit inconsistencies between the attribution rules of *lex specialis* and general international law, the interpretation of the purposes of *lex specialis* is essential for choosing the rules. The commentaries cited the view of the European Court of Human Rights in the *Neumeister* case, which concluded

<sup>61</sup>B. Cheng, ‘Article VI of the 1967 Space Treaty Revisited: “International Responsibility”, “National Activities”, and “The Appropriate State”’, (1998) 26 *Journal of Space Law* 7, at 23–6.

<sup>62</sup>C. J. Robinson, ‘Changing Responsibility for a Changing Environment: Evaluating the Traditional Interpretation of Article VI of the Outer Space Treaty in Light of Private Industry’, (2020) 5 *University of Bologna Law Review* 1, at 14.

<sup>63</sup>See Cheng, *supra* note 61, at 22.

<sup>64</sup>*Ibid.*, at 24.

<sup>65</sup>*Ibid.*, at 25.

<sup>66</sup>See Robinson, *supra* note 62, at 14; see also *ibid.*

<sup>67</sup>See Hobe, Schmidt-Tedd and Schrogl, *supra* note 12, at 114.

<sup>68</sup>See *Commentaries*, *supra* note 58.

that if the application of *lex specialis* would have led to ‘consequences incompatible with the aim and object of the treaty’, the application of the more general provision would be sustained.<sup>69</sup> Accordingly, if applying *lex specialis* would cause consequences incongruent with the objectives of the regimes, a fallback on general international law is expedient to serve the purposes of the special regime.<sup>70</sup> As mentioned above, strict adherence to Article VI of the OST for attributing malicious cyber activities manipulating space activities would lead to unjust results. The attribution rules of general international law may, thus, serve as complements.

Chapter IV of the ARSIWA embraces three different situations where states are implicated in internationally wrongful acts of others – aid or assistance in the commission of an internationally wrongful act, direction and control exercised over the commission of an internationally wrongful act, and coercion of another state. Among these, the first situation is of particular relevance in the context of malicious cyber activities manipulating space activities. They cannot be directly attributed to the states carrying out space activities manipulated by the malicious actors; however, these states are suspected of facilitating malicious cyber activities because the space activities are used as a tool by the malicious actors to achieve their goals. This is where Article 16 of the ARSIWA could be applied.

Though the norm contained in Article 16 was confirmed as customary in the *Bosnian Genocide* case,<sup>71</sup> its application remains challenging, notably when consensus has not been reached over the definition of aid or assistance. Generally, aid or assistance arises when a state actively provides military, economic, or technical assistance to another.<sup>72</sup> Aust suggests two ways to interpret ‘aid or assistance’ – to refer to the typology of cases and situations, which were surveyed to determine Article 16 as a customary rule and to draw inspiration from primary/special rules on complicity.<sup>73</sup> The first method is not helpful since the relevance of existing precedents with malicious cyber activities manipulating space activities is limited. For the second method, Aust, after analysing the statements by governmental representatives regarding their understanding of the term ‘assistance’ in several international treaties, highlighted the impossibility of establishing a list of abstract criteria for identifying aid or assistance within the meaning of Article 16.<sup>74</sup> Hence, neither of the two methods could be applied to define aid or assistance in the current circumstances.

Nonetheless, the three guidelines on the scope of responsibility for aid or assistance prescribed in Article 16 of the ARSIWA shed light on solving the definitional dilemma. Primarily, the relevant state organ or agency providing aid or assistance must be aware of the circumstances making the conduct of the assisted state internationally wrongful. Second, aid or assistance must be given to facilitate the commission of a particular act and must do so. Third, the completed act must be such that it would have been wrongful had it been committed by the assisting state. The first two guidelines are vital for deciding whether the state responsible for the manipulated space activities provides aid or assistance.

The first guideline requires that the assisting state be aware of the circumstances making the conduct of the assisted state internationally wrongful, reflected in the phrase ‘knowledge of the circumstances of the internationally wrongful act’.<sup>75</sup> Although extensive debates over the subjective element of aid or assistance are spread over the drafting history of the AWSIRA, Article 16 adopted the ‘knowledge of circumstances’ test instead of requiring a more substantial mental element, such as the ‘intention’ of the breaching conduct. Thus, knowledge of the circumstances of

<sup>69</sup>*Ibid.*

<sup>70</sup>B. Simma and D. Pulkowski, ‘Leges speciales and self-contained regimes’, in J. Crawford et al. (eds.), *The Law of International Responsibility* (2010), 139, at 146.

<sup>71</sup>See *Bosnia and Herzegovina v. Serbia and Montenegro* case, *supra* note 35, at 217, para. 420.

<sup>72</sup>V. Lanovoy, ‘Complicity in an Internationally Wrongful Act’, in A. Nollkaemper and I. Plakokefalos (eds.), *Principles of Shared Responsibility in International Law: An Appraisal of the State of the Art* (2014), 134, at 141.

<sup>73</sup>H. P. Aust, *Complicity and the Law of State Responsibility* (2011), at 198.

<sup>74</sup>*Ibid.*, at 200–10.

<sup>75</sup>See *Commentaries*, *supra* note 58, at 156.

the wrongful act suffices to fulfil the subjective requirement for holding the assisting state responsible unless the primary rules breached expressly require a show of intention.<sup>76</sup> An opinion expressed by the UN Legal Counsel regarding the collaboration of the UN mission in the Democratic Republic of Congo and the *Forces Armées de la République démocratique du Congo*, and the *El-Masri* judgment rendered by the European Court of Human Rights illustrate the knowledge of circumstances test.<sup>77</sup> It is proposed that the criteria for ascertaining knowledge of the circumstances of the internationally wrongful act include the notoriety of facts where ‘the circumstances were such as called for some reaction, within a reasonable time’, the particular interests of assisting the state in the region, the geographical proximity, and the nature of the aid or assistance and of the breach itself.<sup>78</sup> These elements may play an important role in proving that the state responsible for the space activities has acquired knowledge of the circumstances of the malicious cyber activities. However, specific characteristics of malicious cyber activities manipulating space activities are worth special attention.

Two situations should be distinguished based on the conditions under which malicious cyber activities enter the purview of states responsible for space activities. Under the first situation, states acquire knowledge of potential malicious cyber activities during their international duties in conformity with Article VI of the OST. For instance, the state responsible for space activities discovers, through its national routine control and supervision measures adopted per international space law, the intrusion of its space systems by malicious actors. However, it allows the vicious operation to happen even if it has the capabilities to suppress it. In this case, except for being charged with providing aid or assistance to the malicious actor, the state shall be directly responsible for failing to ensure the conformity of its national activities in outer space with international space law. Notably, Article III of the OST stipulates that state parties shall carry on activities in the exploration and use of outer space in the interest of maintaining international peace and security. The second situation happens when the state responsible for space activities performs its duties yet acquires knowledge of malicious cyber activities through other sources. Hence, the first requirement for establishing the responsibility for providing aid or assistance is met. To differentiate the two situations, the primary issue of ascertaining the scope and content of a state’s international obligations arises. It is paramount in the context of the knowledge of circumstances test for identifying the nature of the possible international responsibility, whether direct or indirect.

The second guideline is that aid or assistance must be given to facilitate the commission of the wrongful act and must actually do so.<sup>79</sup> There is no requirement that the aid or assistance should be essential to the performance of the wrongful act,<sup>80</sup> and it would be sufficient to have the former contribute significantly to the latter.<sup>81</sup> The aid or assistance does not have to constitute a *conditio sine qua non* (an indispensable condition) for the performance of the wrongful act, or the assisting state would be likely to assume an independent direct responsibility.<sup>82</sup> It is only required that the aid or assistance should have made the wrongful conduct easier to commit. Thus, Article 16 does not reflect the differences in substance and degree,<sup>83</sup> which is essential to distinguish it from joint direct responsibility. A minimum level of involvement in wrongful conduct could be considered as providing aid or assistance, even if the act plays a trivial and dispensable part. Hence, any space activities facilitating the achievements of malicious actors’ purposes could be considered aid or assistance, regardless of the role that the space activities play in the incident. The unreasonableness

<sup>76</sup>See Lanovoy, *supra* note 72, at 150.

<sup>77</sup>*Ibid.*, at 153–5.

<sup>78</sup>*Ibid.*, at 155.

<sup>79</sup>*Ibid.*; see Commentaries, *supra* note 58, at 156.

<sup>80</sup>See Aust, *supra* note 73, at 197.

<sup>81</sup>See Commentaries, *supra* note 58.

<sup>82</sup>See Aust, *supra* note 73, at 213.

<sup>83</sup>See Crawford, *supra* note 34, at 338.

of this corollary is significantly reduced by the subjective aspect of aid or assistance. Although hard to prove, the intention to facilitate the wrongful conduct of the assisting state is critical for holding the state responsible.<sup>84</sup>

In addition, omissions are not explicitly excluded from the scope of aid or assistance. Though the *Bosnian Genocide* case demonstrated that complicity through omission is inconceivable,<sup>85</sup> the rule is not ingrained and there are chances that omission constitutes aid or assistance, as illustrated by the *Corfu Channel* case.<sup>86</sup> A precondition for this identification lies in an international obligation to act. In malicious cyber activities manipulating space activities, the omission of the state responsible for the space activities may constitute aid or assistance if the state curbs the malicious cyber activities and the adverse consequences; thus, reverting the conundrum to determine the scope and content of international obligations of the state responsible for space activities.

#### 4.2 Attributing to a plurality of directly responsible states

There are chances that states' respective and independent breaches of international law contribute to a single malicious cyber activity. The basic principle of attribution for this category of joint and collective conduct is that all states are individually and independently responsible for their own acts.<sup>87</sup> However, two sub-scenarios can occur, implying the varied ways of applying attribution rules. First, the state responsible for space activities is unaware of the malicious actor's intrusion into its space systems. If the state fails to perform its international duties, allowing the malicious actors to exploit the vulnerabilities of its space system then the state should bear direct international responsibility for the OST breach. However, if the state fulfils its international obligations yet fails to perceive the cyber intrusions then no international responsibility should be imposed upon the state. Thus, the key to settling the responsibility issue of this sub-scenario lies in determining the scope and content of states' international obligations for their national activities in outer space.

Second, the activities in outer space are national activities of a state, which is aware of the ongoing malicious cyber activities without the intention to facilitate the wrongful act. The space systems and objects could be assimilated into tools for realizing malicious cyber activities. If a satellite is used to transfer orders commanded by the malicious actor then the satellite constitutes vital support for the incident. In this case, whether the state has fulfilled its international obligations is essential, while attribution is not difficult to decide. This situation is similar to the case where cyber infrastructures, including undersea fibre-optic cable systems, are utilized to transfer malicious actors' orders in terrestrial malicious cyber activities where due diligence may play a role.

Hitherto, the scope and substantial obligations of due diligence in cyberspace remain under discussion. The due diligence obligation was defined in the *Corfu Channel* case as an international obligation requiring that every state should 'not to allow knowingly its territory to be used for acts contrary to the right of other states'.<sup>88</sup> This interpretation relied largely upon jurisprudence in the law of armed conflict;<sup>89</sup> however, it was embraced in several branches of international law. Following subsequent judicial decisions, the due diligence principle has evolved into a customary norm, mirrored in Article 3 of the ILC's 2001 Draft Articles on Prevention of Transboundary

<sup>84</sup>*Ibid.*

<sup>85</sup>See *Bosnia and Herzegovina v. Serbia and Montenegro*, *supra* note 35, at 222, para. 432.

<sup>86</sup>See Aust, *supra* note 73, at 225–7.

<sup>87</sup>See Crawford, *supra* note 34, at 334.

<sup>88</sup>*Corfu Channel case (United Kingdom of Great Britain and Northern Ireland v. Albania.)*, Judgment of 9 April 1949, [1949] ICJ. 4, at 22.

<sup>89</sup>A. Berkes, 'The Standard of "Due Diligence" as a Result of Interchange between the Law of Armed Conflict and General International Law', (2018) 23 *Journal of Conflict and Security Law* 433, at 433.

Harm from Hazardous Activities (Draft).<sup>90</sup> Nonetheless, state practice implies doubts about its status as a customary norm, notably reflected in the stagnation of the Draft's progress into a binding document.<sup>91</sup> Furthermore, even if the due diligence principle is accepted as a customary norm, notwithstanding the clarifications of the concrete due diligence obligations in different branches of international law,<sup>92</sup> it cannot be deduced that similar binding obligations to prevent and redress harm exist in cyberspace.<sup>93</sup> The due diligence obligations in cyberspace have gathered scholarly views without consensus.

International efforts have been made to address the conundrum of the due diligence principle in cyberspace. Six Groups of Governmental Experts (GGE)<sup>94</sup> have convened following the UN's placement of the cyber activities issue on its agenda since 1998<sup>95</sup> and issued reports representing consensus over relevant legal issues. The 2013 report explicitly expressed views on cyber due diligence and enunciated that 'states must not use proxies to commit internationally wrongful acts and must ensure that their territories are not used by non-state actors for unlawful use of the information and communications technologies (ICTs)'.<sup>96</sup> The 2015 report added that states should ensure that their territory 'is not used by non-state actors to commit such acts'.<sup>97</sup> According to the two reports, due diligence obligations imposed on states concern the malicious cyber activities conducted by both state and non-state actors, exerting pressure on the states. This perspective is reflected in Norm 13(c) of the final report of the GGE,<sup>98</sup> underlining that states should not knowingly allow their territory to be used for internationally wrongful acts using ICTs. This indicates the prerequisites of states' due diligence obligations in cyberspace – the state has constructive knowledge of malicious cyber activities and internationally wrongful acts happening on or through the state's territory. However, even when these preconditions are met, issues like the measures to be undertaken by a state and their effectiveness are not tackled.

Notwithstanding the efforts exerted to tackle the cyber due diligence issues, some states remain reluctant to accept, even against applying, the due diligence principle in cyberspace.<sup>99</sup> This is understandable since applying the principle would compel states to improve their ICT capacities, which may not align with their current development plans. Similarly, strict adherence to the due diligence principle in malicious cyber activities manipulating space activities would impose excessive pressure on the states carrying out space activities. Particularly, considering the high costs of adopting cyber security and awareness measures, due diligence obligations would increase the inputs of commercial space activities and set up obstacles for this promising industry.

<sup>90</sup>A. Coco and T. de Souza Dias, "Cyber Due Diligence": A Patchwork of Protective Obligations in International Law', (2021) 32 EJIL 771, at 776; ILC, *Draft Articles on Prevention of Transboundary Harm from Hazardous Activities, with commentaries*, UN Doc. A/56/10 (2001), 144, at 154.

<sup>91</sup>See E. T. Jensen and S. Watts, 'Cyber Due Diligence', (2021) 73 *Oklahoma Law Review* 645, at 679–80.

<sup>92</sup>See Coco and de Souza Dias, *supra* note 90.

<sup>93</sup>T. Dias and A. Coco, *Cyber Due Diligence in International Law*, Project Report, Oxford Institute for Ethics, Law and Armed conflict, at 163, available at [www.elac.ox.ac.uk/wp-content/uploads/2022/03/finalreport-bsg-elac-cyberduediligenceininternationalallawpdf.pdf](http://www.elac.ox.ac.uk/wp-content/uploads/2022/03/finalreport-bsg-elac-cyberduediligenceininternationalallawpdf.pdf).

<sup>94</sup>United Nations Office for Disarmament Affairs, Factsheet: Developments in the Field of Information and Telecommunications in the Context of International Security, July 2019, available at [front.un-arm.org/wp-content/uploads/2019/07/Information-Security-Fact-Sheet-July-2019.pdf](http://front.un-arm.org/wp-content/uploads/2019/07/Information-Security-Fact-Sheet-July-2019.pdf).

<sup>95</sup>Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/RES/53/70 (1999).

<sup>96</sup>Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/68/98 (2013).

<sup>97</sup>Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/70/174 (2015).

<sup>98</sup>Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, UN Doc. A/76/135 (2021).

<sup>99</sup>I. Y. Liu, 'The Due Diligence Doctrine under Tallinn Manual 2.0', (2017) 33 *Computer Law & Security Review* 390, at 395.



Applying the due diligence principle to malicious cyber activities manipulating space activities should, thus, be extremely prudent.

#### 4.3 Sub-conclusion

States responsible for manipulated space activities may contribute to the incident and bear international responsibility. For states responsible for space activities implicated in malicious cyber activities, it is paramount to choose the applicable law for attribution where a peculiarity test would help. The attribution provisions in Article VI of the OST may not always be appropriate, leading to a possible application of general international law, particularly the attribution rules on aid or assistance in the commission of an internationally wrongful act, crystallized in Article 16 of the ARSIWA. Hence, the scope and substantive content of international obligations imposed on states responsible for manipulated space activities are vital for deciding whether the state should be held responsible for aid or assistance.

States responsible for space activities may contribute to malicious cyber activities manipulating space activities by directly breaching international obligations. To hold those states which are aware of the ongoing incident responsible, examining the states' due diligence obligations would be inevitable. However, without an international consensus on its content, a careful application of the due diligence principle should be practised as it may lead to unexpected repercussions.

### 5. Scenario three: Malicious activities from outer space

Scenario three may have different sub-scenarios, especially when the number of states involved varies. The first sub-scenario presupposes that the state of nationality of the malicious actor and the responsible state for the space activities are different. Following the development of space tourism, more than one state may participate in a single space mission. For instance, a company based in state A runs a space tourism business and buys launching services from state B to send tourists from state C into outer space. The company signs an agreement with state D to visit the space station that D operates. In this case, four states are involved in the space mission during which malicious cyber activity is conducted; hence, all four states could be held internationally responsible. In the second sub-scenario, the state of nationality of the malicious actor and the responsible state of the space activities during which the MCASA is conducted are identical. Only one state is involved and the attribution is relatively easy to establish. The attribution rules of international space law suffice.

The sub-scenarios share similarities in that the malicious cyber activities are conducted during space activities or even planned as an integral part of a space mission. However, differences exist, as the predicament of attribution is present in the first sub-scenario where malicious cyber activities from outer space could be attributable to a plurality of states, which will be the focus of discussion in this section.

According to the *lex specialis derogat legi generali* principle, applying the attribution rules of the *corpus iuris spatialis* (space treaties) seems reasonable. However, as analysed in Section 4, the proposed approaches for interpreting 'national activities' are inappropriate. The most supported interpretation of 'national activities' indicates the state exercising jurisdiction over the space object involved, precluding the possibility of several responsible states. The states of nationality of the malicious actor and the space tourism company would be exempted from any legal consequence even if the individual and the company were exercising elements of the governmental authority of the state, meeting the requirements of Article 5 of the ARSIWA.

The absence of authoritative guidance on the proper interpretation of 'national activities' provides states the discretion to determine the concept's scope, resulting in widely different

national implementation mechanisms of Article VI of the OST.<sup>100</sup> In the context of malicious cyber activities from outer space, this situation would lead to uncertainties in identifying the responsible state. Injudiciously applying the attribution rules in Article VI to malicious cyber activities from outer space would give rise to undesirable consequences contrary to the purpose of the international space law. Moreover, there are lacunae in Article VI regarding joint or collective conduct, which necessitates referring to the general international law.

Two categories of joint or collective conduct can be distinguished in scenario three – where states are implicated in malicious cyber activities from outer space and where they are directly responsible for breaching international obligations.

### **5.1 *Attributing to the states implicated in the malicious cyber activities***

The absence of relevant rules of international space law dealing with this category of joint and collective conduct necessitates referring to the attribution rules of general international law, crystallized in Chapter IV of the ARSIWA. The dilemma of applying Article 16 is identical to that of applying this article to the states responsible for space activities implicated in malicious cyber activities manipulating space activities.

There is no clear definition of ‘aid or assistance’. According to Aust, lessons could be drawn from the typology of cases and situations.<sup>101</sup> International practice shows that a state allowing its territory to be used by another state, which assembles its troops and conducts its attack from the former’s territory, is considered aid or assistance.<sup>102</sup> The malicious cyber activities from outer space share similarities with this case in that the physical sphere of carrying out the wrongful act is provided by a state different from the state of nationality of the malicious actor. Similarly, the state launching the malicious actor to outer space is likely to be held imputable. However, their circumstances are different. In conventional conflicts, the assisting state has geographical advantages so that the use of its territory by the attacking state would substantially facilitate an attack against a neighbouring state. However, the locales of malicious cyber activities, randomly selected, seldom matter. Whether an unauthorized cyber activity is conducted on Earth or in outer space does not affect its consequences, making the ‘space’ factor trivial for malicious cyber activities from outer space. Thus, providing a place for carrying out malicious cyber activities could hardly be considered aid or assistance. In addition, as Aust underlined, a list of cases will not be able to provide normative guidance on the concept of aid or assistance,<sup>103</sup> and a single case in international practice does not necessarily lead to the conclusion that an act should be identified as an analogous incident. The shortcoming of the second way has been submitted by Aust.<sup>104</sup> States will need time and occasions to express their understanding of aid or assistance. Both methods are enlightening for identifying aid or assistance in malicious cyber activities from outer space; however, they do not consider their peculiarities.

Concerning the subjective aspect of aid or assistance – knowledge of circumstances of the malicious cyber activities from outer space – two situations could be distinguished. An illustrative case of the first situation, under which states become aware of the malicious cyber activities during their international duties, could be as follows: the state responsible for the spacecraft hosting space travellers discovers, through its national routine control and supervision measures adopted per international space law, a malicious cyber activity by one of the travellers on board; however, it ignores the vicious operation even if it has the capabilities to stop it. The state responsible for the

<sup>100</sup>F. G. von der Dunk, ‘The Origins of Authorisation: Article VI of the Outer Space Treaty and International Space Law’, in F. G. von der Dunk (ed.), *National Space Legislation in Europe: Issues of Authorisation of Private Space Activities in the Light of Developments in European Space Cooperation* (2011), 3, at 16.

<sup>101</sup>See Aust, *supra* note 73, at 198.

<sup>102</sup>*Ibid.*

<sup>103</sup>*Ibid.*, at 200.

<sup>104</sup>*Ibid.*, at 200–10.

spacecraft shall bear direct responsibility for failing to carry out its space activities in the interest of maintaining international peace and security. The second situation is where the states involved in space activities have performed their duties; however, acquired knowledge of the malicious cyber activity, is likely to fulfil the subjective requirements of aid or assistance. Deciding the scope and content of states' international obligations is, therefore, vital for differentiating the two situations, which may lead to different international responsibilities, direct or indirect.

The existence of a causal link between the aid or assistance and the wrongful act is required.<sup>105</sup> Per Article 16 of the ARSIWA, a minimum level of participation in wrongful conduct could be considered as providing aid or assistance. The content of the aid or assistance and the intention of the assisting state decide the nature of the conduct,<sup>106</sup> necessitating a case-by-case assessment. Thus, whether the act of the state involved in the space activities constitutes aid or assistance remains uncertain as no uniform criteria could be established in this regard. The solution to this dilemma may lie in various factors, including the intention of the malicious actor, the technical environment on board, and the targets and purposes of the malicious cyber activity. These must be assessed according to the specific circumstances of each case.

## 5.2 *Attributing to several states directly breaching international obligations*

A rigid adherence to international space law or general international law attribution in the case of a direct breach of international obligations by several states participating in one space mission would lead to undesirable consequences. As analysed above, the precipitate application of international space law would lead to unwanted effects, such as intimidating the development of commercial space activities or unreasonably excluding the responsibility of some states. However, if the attribution rules of general international law were applied, without successfully establishing an adequate link between the malicious cyber activity and the states involved in the space activities in conformity with Articles 4–11 of the ARSIWA, none of the states may be held responsible. Following this conclusion, the challenges of establishing an appropriate attribution standard in the cyber sphere resurge. As it is during a space mission, which should be governed by international space law, that malicious cyber activities are carried out, if no state involved in the space activity can be held responsible due to attribution issues, it would be incompatible with the purposes of Article VI of the OST to ensure the rights of the injured parties.

This dilemma may be settled through a four-pronged approach. The first pillar of the approach is identifying the attributable states in a phased manner. A space trip could be divided into three phases: (i) the entering phase, where the space travellers are sent from the Earth to outer space; (ii) the staying phase, where the travellers stay in a spacecraft in outer space; and (iii) the return phase, where the travellers return from outer space to the Earth in a return capsule. Different states are implicated in the three phases and the attribution could be decided based on the phase in which the malicious cyber activity was conducted. For instance, if malicious cyber activity from outer space happens during the entering phase, the state responsible for the spacecraft where the travellers stay and the state providing the return capsule shall be directly excluded from the international responsibility issues.

The second pillar indicates a broader interpretation of the term 'national activities'. To ensure that all the activities in outer space become the responsibility of a state for the protection of the victims,<sup>107</sup> 'national activities' should be understood in a way that they are the national activities of all states exercising territorial, quasi-territorial, or personal jurisdiction over them. Article VI does not provide for the cases of multiple responsible states; however, it does not explicitly preclude the imputation of a wrongful act to several states. Thus, theoretically, all the states involved in a

<sup>105</sup>See *Commentaries*, *supra* note 58.

<sup>106</sup>See Lanovoy, *supra* note 72, at 144; I. Brownlie, *System of the Law of Nations: State Responsibility Part 1* (1983), at 191.

<sup>107</sup>See Cheng, *supra* note 61, at 23.

certain phase of the space mission could be held internationally responsible for malicious cyber activity during that phase, leading to the above-illustrated unreasonable results.

Thus, it would be logical to give all the involved states a chance to prove their innocence, and the burden of proof should be shifted to the states to demonstrate that they have fulfilled their international obligations, which is the essence of the third pillar. Any state, which has successfully proved that it has fulfilled its international obligations related to the space mission shall be exempted from international responsibility arising out of the malicious cyber activities conducted during the mission.

Following the second and third pillars, the fourth pillar specifies the extent and content of the international obligations of the state involved. Though this pillar concerns the primary rules of the international responsibility regime, it is pivotal for the entire approach. Per Articles III and VI of the OST, all states should carry on activities in the exploration and use of outer space, including the Moon and other celestial bodies, in accordance with international law and shall bear international responsibility for national activities to ensure that they are carried out in conformity with the provisions outlined in the OST. While the exact content and extent of the international obligations are not precisely defined in the OST, many states have made efforts to ensure the conformity of their space activities, including launching activities, by enacting national laws and establishing licensing regimes.<sup>108</sup> However, although almost all states exercise both territorial and personal jurisdiction over their national legislations,<sup>109</sup> and authorization is a prerequisite for all legal persons under their jurisdiction willing to carry out space activities, the specific legal requirements for space tourism companies and private space travellers are seldom defined. With the space tourism boom, states would be required to extend their control and supervision measures to individuals, especially private space travellers. The legislation about Antarctica in the UK, requiring all persons wishing to enter or remain in Antarctica on a British expedition to acquire a permit,<sup>110</sup> may have referential significance in this respect. Following this approach, the UK could supervise the expedition and the participants, regardless of their nationalities. This tailored supervision for expeditions to Antarctica could serve as a starting point for states to supervise private space tourists. All space tourism companies and the participants of a space trip must get a license or a permit to run or join a space travel mission. Furthermore, the requirements for granting licenses for space tourism activities should be prudently designed to avoid risks caused by persons on board. These national measures, reasonably designed and implemented, may be taken as evidence for a state to demonstrate that it has done its duties.

### 5.3 Sub-conclusion

International space law cannot cope with attributing malicious cyber activities from outer space because its precipitate application would lead to undesired effects incongruent with the objectives of the *corpus juris spatialis* (space treaties), and international space law does not envisage the situation of multiple states being responsible for an internationally wrongful act. The rules of general international law on attributing joint and collective conduct could be complementary.

For cases with indirect responsibility, a peculiarity test should be introduced to determine the nature of the activity, that is, whether it is spatial or terrestrial. The causal link between the aid or assistance and the malicious cyber activity should be assessed based on several factors, including

<sup>108</sup>UNOOSA, 'National Space Law', available at [www.unoosa.org/oosa/en/ourwork/spacelaw/nationalspacelaw/index.html](http://www.unoosa.org/oosa/en/ourwork/spacelaw/nationalspacelaw/index.html); see R. S. Jakhu (ed.), *National Regulation of Space Activities* (2010); K. Abhijeet, 'State Practices Regarding International Responsibility for National Activities in Outer Space', (2020) 44 *Journal of Space Law* 352, at 366–70.

<sup>109</sup>See Abhijeet, *ibid.*, at 366.

<sup>110</sup>Antarctic Act 1994, available at [www.legislation.gov.uk/ukpga/1994/15#:~:text=An%20Act%20to%20make%20new%20provision%20in%20connection,and%2090%20West%20longitude%3B%20and%20for%20connected%20purposes](http://www.legislation.gov.uk/ukpga/1994/15#:~:text=An%20Act%20to%20make%20new%20provision%20in%20connection,and%2090%20West%20longitude%3B%20and%20for%20connected%20purposes); C. J. Bastmeijer, 'Implementing the Antarctic Environmental Protocol: Supervision of Antarctic Activities', (2003) 11 *Tilburg Law Review* 407, at 417–18.

the malicious actor's intention, the technical environment on board, and the targets and purposes of the cyber activity. A four-pronged approach has been proposed for cases that may give rise to direct responsibility to several states, including a phased analysis of malicious cyber activities from outer space, a broader interpretation of 'national activities,' shifting the burden of proof, and specifying the extent and content of the international obligations of the states whose space activities are involved.

## 6. Conclusion

The complexities of MCASAs obscure the nature of the malicious conducts. Whether they are space or terrestrial activities determines the applicable attribution rules. If these malicious cyber activities are identified as space activities, the international space law shall apply based on the *lex specialis derogat legi generali* principle. However, there are some circumstances that Article VI of the OST does not envisage or where the application of this article would lead to results contrary to the purposes of the Treaty. In such cases, general international law is likely to play a complementary role.

Even with two sets of attribution rules, legally attributing MCASAs would remain challenging. This study proposes the following approaches for tackling different predicaments in various hypotheses:

1. For malicious cyber activities against terrestrial systems, the virtual control test would be appropriate in most cases; however, a stricter standard, such as the effective control test, should be applied when the victim state tries to take retaliatory actions.
2. For malicious cyber activities manipulating space activities, introducing a peculiarity test and determining the extent and content of the international obligations born by states involved in space-related activities are vital. In addition, applying the due diligence principle to malicious cyber activities manipulating space activities should be prudent.
3. For malicious cyber activities from outer space, which may give rise to direct responsibility, a four-pronged approach should be adopted, including a phased analysis of the incident, a broader interpretation of 'national activities,' shifting the burden of proof, and specifying the extent and content of international obligations of the states whose space activities are involved.
4. For malicious cyber activities from outer space, which may give rise to indirect responsibility, a peculiarity test should be introduced to determine the nature of the activity, that is, whether it is spatial or terrestrial. The causal link between the aid or assistance and the malicious cyber activity should be assessed based on several factors, including the intention of the malicious actor, the technical environment on board, and the targets and purposes of the malicious cyber activity.

All the discussions in this article are based on the premise that MCASAs violate international law. However, this does not hold for all malicious cyber activities. MCASAs may be conducted in various forms, including spoofing and hacking attacks on communication networks, targeting control systems or mission packages, and attacking the ground infrastructure.<sup>111</sup> They may include malignant conducts amounting to 'use of force' or 'armed attack'. However, the most frequent malicious cyber activities, such as spoofing or invading the control systems without further actions, are usually trivial and hard to detect. They are wandering or below the threshold of breaching international law. Coping with these acts could be a more vexing issue in the future.

<sup>111</sup>D. Livingstone and P. Lewis, 'Space, the Final Frontier for Cybersecurity?', *International Security Department*, September 2016, available at [www.chathamhouse.org/sites/default/files/publications/research/2016-09-22-space-final-frontier-cybersecurity-livingstone-lewis.pdf](https://www.chathamhouse.org/sites/default/files/publications/research/2016-09-22-space-final-frontier-cybersecurity-livingstone-lewis.pdf).

International space law may play a role in determining states' international obligations in the case of MCASAs; however, it proves to be incapable towards these acts. Cybersecurity norms would be more appropriate for dealing with this dilemma. Absent international binding cybersecurity norms and the GGE reports represent states' common view regarding responsible state behaviour in cyberspace. The 2021 report contains the norms that have been agreed upon and adds a layer of understanding to them. They are supplemented by the recommendations in the Open-Ended Working Group report, which provides additional guidance on what constitutes responsible state behaviour regarding ICTs usage.<sup>112</sup> Although the norms are voluntary and non-binding, states consider them as guidance regarding the application of international law in cyberspace.<sup>113</sup> The development of international norms on cyberspace will contribute to identifying states' international obligations related to cyberspace and help tackle cyber activities that are currently difficult to evaluate.

From a practical perspective, states are reluctant to clarify the ambiguous terminology used in existing space treaties and adopt new space treaties. The developing international norms regarding responsible state behaviour in cyberspace are yet to be crystallized in binding instruments or recognized as customary international law. This is unfavourable for tackling the attribution dilemma since states' international obligations in the context of malicious cyber activities are difficult to determine. The concretization of abstract principles of international space law and standardization of states' responsible behaviour in cyberspace is a significant topic. Bottom-up soft law approaches may provide an option to make progress in law-making in certain relevant areas.<sup>114</sup>

<sup>112</sup>Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security. UN Doc. A/75/816 (2021).

<sup>113</sup>H. Moynihan, 'The Application of International Law to State Cyberattacks: Sovereignty and Non-intervention', *International Law Programme*, December 2019, available at [www.chathamhouse.org/sites/default/files/publications/research/2019-11-29-Intl-Law-Cyberattacks.pdf](http://www.chathamhouse.org/sites/default/files/publications/research/2019-11-29-Intl-Law-Cyberattacks.pdf).

<sup>114</sup>J. P. Jurich, 'Cyberwar and Customary International Law: The Potential of a Bottom-up Approach to an International Law of Information Operations', (2008) 9 *Chicago Journal of International Law* 275, at 295; P. Martinez, 'The Role of Soft Law in Promoting the Sustainability and Security of Space Activities', (2020) 44 *Journal of Space Law* 522, at 545.