Centro Alti Studi Difesa

Scuola Superiore Universitaria

STRATEGIC LEADERSHIP JOURNAL

CHALLENGES FOR GEOPOLITICS AND ORGANIZATIONAL DEVELOPMENT

Volume IV – Dicembre 2024

Centro Alti Studi Difesa – Scuola Superiore Universitaria

Direzione e Redazione Palazzo Salviati
Piazza della Rovere, 83, 00165 – Roma
www.casd.it
Tel 06 4691 23208 – e-mail: irad.usai@casd.difesa.it

ISSN 2975-0148 – ISBN 9791255150787

INDICE

Elisa Leoni
Ph.D. Student at the School Of Advanced Defence Studies (CASD/SSUOS) - University of Turin (UNITO), in Defence & Security Studies, curriculum: Legal studies for innovation

EXPLORING THE INTERCONNECTION BETWEEN SPACE AND CYBERSPACE: THE DUE DILIGENCE PRINCIPLE AS A TOOL OF INTERNATIONAL LAW TO COUNTER CYBERATTACKS ON SPACE SYSTEMS

ABSTRACT

Il presente contributo si propone di esaminare il principio della due diligence come strumento di diritto internazionale per contrastare e condannare gli attacchi cibernetici ai segmenti di terra dei sistemi spaziali. Dopo una panoramica sulla crescente interconnessione tra spazio e cyberspazio, farà seguito un"analisi del principio della due diligence, sia dal punto di vista del diritto internazionale, sia nella sua applicazione al dominio cibernetico. Questo approccio teorico verrà infine applicato al caso di studio relativo all"attacco cibernetico del 24 febbraio 2022, che ha compromesso i servizi di comunicazione satellitare della compagnia americana ViaSat.

This paper advocates for the due diligence principle as a vital tool in International Law to tackle and condemn cyberattacks targeting the ground segments of space systems. It begins by exploring the growing connection between space and cyberspace, before examining how the due diligence principle is understood in International Law. The discussion then shifts to how this principle can be interpreted and applied specifically within the cyber domain. Finally, this framework is used to analyse the February 24, 2022, cyberattack on the satellite communication services of the American company ViaSat.

Introduction

The Russian-Ukrainian war has opened the eyes of the international community to the essential nature of satellite services, not only in the military context but also in our daily lives. Satellites are not only critical infrastructures[1], but also serve as the foundation for numerous other essential systems, creating a potential single point of failure for a wide range of sectors[2]. Space systems are indispensable for both civilian and military applications, supporting activities that are integral to the functioning of modern society. For instance, the financial sector relies on accurate Positioning, Navigation, and Timing (PNT) data to ensure precise timestamping of transactions. The transportation and logistics sectors depend on satellite-based location data for

[1] For instances the European Union classifies space as European Critical Infrastructure in its Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC.

[2] United States General Accounting Office (GAO) Report, CRITICAL INFRASTRUCTURE PROTECTION Commercial Satellite Security Should Be More Fully Addressed, 2002.

tracking shipments, optimising routes, and managing supply chains efficiently. In emergency contexts, satellite communications are vital for ensuring reliable and resilient communication during disaster recovery, search and rescue operations, and emergency response coordination[3]. Space systems also contribute to advancements in entertainment and research, highlighting their multifaceted importance. Moreover, they support military command and control operations and provide internet connectivity to remote and underserved regions around the globe.
Nevertheless, the complexity of these systems often results in inadequate cybersecurity measures, further exacerbated by the lack of comprehensive international policies to strengthen their resilience[4].
What the conflict has also underscored is the direct interconnection between space and cyberspace. This interweaving stems from the fact that, on one hand, there is a domain geographically distant from Earth, namely space, and on the other, a domain capable of overcoming any distance, namely cyberspace. This interconnection entails and will continue to entail an increase in cyber risks and threats directed toward outer space, which will consequently impact activities carried out on Earth. From the International Law perspective, a principle that could limit these threats by preventing and particularly condemning them is the due diligence principle. Unfortunately, its application in cyberspace is not yet considered customary, but assisting in its process of application by highlighting its strengths and weaknesses will certainly help in the development of state practice in this area. Applying the due diligence obligation to real-world events, providing evidence of possible shortcomings arising from this process, and clarifying the application itself is the primary objective of this article, which is organized as follows. Section 1 examines the characteristics and consequences of the interconnection between space and cyberspace. Subsequently, section 2 provides a legal analysis of the due diligence obligation in International Law, tracing its origins and contemporary interpretation by the international community. Subsection 2.1 attempts to apply the principle to the cyber domain, focusing on its legal characteristics. Finally, Section 3 promotes the application of the due diligence principle to the ViaSat cyberattack case study. To achieve this, subsection 3.1 delves into the technical characteristics of the attack, explained in simplified terms, while subsection 3.2 attempts to attribute the alleged violation of the due diligence obligation in cyberspace to the Russian Federation. In the concluding section, the advantages and shortcomings of applying the principle under analysis are discussed based on the elements revealed throughout the examination.

1. The increasing interconnection between space and cyberspace

It can be argued that there is a significant interconnection between space and cyberspace, which may expose satellite technologies to cyber threats. Indeed, as has been declared by the Commander of the U.S. Space Force"s Space Operations Command, Lt. Gen. Stephen Whiting: «Cyberspace is the soft underbelly of our global space networks»[5]. Accordingly, the main threat for space assets it is

[3] BACE B. - YASIR G. - UNAL T., *Law in Orbit: International Legal Perspectives on Cyberattacks Targeting Space Systems,* in «*Telecommunications Policy*» 48 (2024) p.2. https://doi.org/10.1016/j.telpol.2024.102739.

[4] VARADHARAJAN V. - SURI N., *Security challenges when space merges with cyberspace*, in «Space Policy», 67 (2024), http://dx.doi.org/10.1016/j.spacepol.2023.101600.

[5] ERWIN S., *Space Force to shore up cybersecurity as threats proliferate*, Space News, 2022, Space Force to shore up cybersecurity as threats proliferate - SpaceNews.

represented by cybers-attacks[6] which with rapidity, unpredictability and easiness, can partially or completely compromise the function of space systems.
This vulnerability was not identified only recently. As demonstrated in the Martinovic and Pavur Manual, over the past 60 years there have been more than a hundred cases of malicious cyberattacks targeting satellites or, more generally, space systems[7]. One notable example occurred in 1998, when a group of hackers managed to take control of the German-American ROSAT X-Ray satellite, instructing it to orient its panels towards the sun provoking irreparable damage to the satellite's optical sensors[8]. In recent years, a notable example is the 2014 cyberattack on a U.S. weather satellite, which caused significant disruption to satellite feeds[9] and impacted various associated websites[10]. Regarding the types of cyberattacks targeting satellite systems, these threats include various methods aimed at different components. Common attacks involve unauthorized attempts to gain command-and-control over satellites, enabling operational disruption. Interception of sensitive data compromises the confidentiality and integrity of communications, while denial-of-service attacks can render systems inoperable, disrupting services[11]. Ransomware attacks block access to critical systems until a ransom is paid, delaying civilian and military operations[12]. Additionally, *spoofing*[13], *jamming*[14] and *hacking* target the link segment, undermining the reliability and security of communications between the space and ground segments. Moreover, the fact that cyberattacks are relatively inexpensive encourages their use by non-state actors who, over the past decades, have increasingly played a prominent role in launching cyberattacks against both States and industries. This growing involvement of non-state actors, often operating with limited resources, but with substantial technical expertise, has amplified the threat landscape, making critical infrastructures particularly vulnerable to disruption and exploitation. For example, the 2007 cyberattacks on Estonia, widely attributed to Russian patriotic hackers, crippled government,

---

6 Cyberattacks are defined by NATO as an act or action initiated in or through cyberspace to cause harmful effects. Source: NCIA | Cyber Security (nato.int).

7 PAVUR J. - MARTINOVIC I., *SOK: Building a Launchpad for Impactful Satellite Cyber-Security Research*, Oxford University, 2020, 2010.10872 (arxiv.org).

8 SUWIJAK C. - LI S., *Global Internet Access from the Low Earth Orbit: Legal Issues regarding Cybersecurity in Outer Space*, in «Journal of East Asia and International Law» (15/No.1), 2022, p.100.

9 Satellite Feeds: The term "feed" refers to a transmission, often live, carried out by a satellite and aimed at supplying one or more television networks. These technical connections are used to route services or enable live broadcasts from distant locations. Source: http://www.scaistar.com/guide/feed/feed01.htm#:~:text=Si%20definisce%20con%20il%20termine, la%20diretta%20da%20luoghi%20lontani.

10 *Ibidem*.

11 KAVALLIERATOS G. - KATSIKAS S., *An exploratory analysis of the last frontier: A systematic literature review of cybersecurity in space*, in «International Journal of Critical Infrastructure Protection», 43 (2023), An exploratory analysis of the last frontier: A systematic literature review of cybersecurity in space - ScienceDirect.

12 BACE B. - YASIR G. - UNAL T., *Law in Orbit: International Legal Perspectives*..op. cit. p. 3.

13 Spoofing: A type of cyberattack used to falsify (from the English verb "to spoof") various types of information, such as the sender of a message, in order to deceive the recipient into believing that the messages originate from known, trustworthy, or unsuspected sources. This type of attack typically leverages social engineering techniques. Source: CSIRT, National Cyber Security Agency, Glossario - CSIRT Italia.

14 Jamming is an electronic attack against wireless communications, affecting the availability of the communication medium by producing interference that prevents the effective reception of the signal. Source: CyCon_2024_book.pdf (ccdcoe.org).

financial, and media services for weeks[15], highlighting how non-state actors are considered important players in the cyber domain.
At the international level, NATO has increasingly recognized the importance of cyber and space domains. Regarding cyberspace, NATO designated it as an operational domain at the 2016 *Warsaw Summit*[16] and, in 2021, acknowledged that significant malicious cyber activities might, under certain circumstances, constitute an armed attack warranting the invocation of Article 5 of the *North Atlantic Treaty*[17](on a case-by-case basis)[18]. At the 2023 *Vilnius Summit*, Allies endorsed a concept to enhance cyber defence"s role in deterrence and launched the Virtual Cyber Incident Support Capability (VCISC) to assist Nations in mitigating major cyber incidents[19]. As for space, NATO declared it a new operational domain at the 2019 *London Summit*[20]. In 2021, leaders stated that attacks "to, from, or within space" could trigger Article 5[21]. The 2023 *Vilnius Summit* emphasized integrating space into joint operations and enhancing data sharing[20]. Most recently, *NATO"s 2024 Summit* highlighted its commitment to a commercial space strategy[22] by engaging industry representatives[23].The relevant fact is that NATO has not only shown interest in space and cyberspace as separate domains, but also in the interconnection between them. Indeed, at the *Madrid Summit* held in July 2022, the integration between cyber operations conducted in cyberspace and the real effects produced in the space environment was established[24]. To better explain, during the Summit it was stated that threats originating from cyberspace can pose real risks to both orbital and terrestrial components, seriously endangering business continuity in the space context[25]. In fact, the primary concern arising from this intersection is that cyber-attacks could render space assets unusable. As already mentioned, these assets are especially crucial in the military context, where they play a central role in

---

15 OTTIS R., *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective*, NATO Cooperative Cyber Defence Centre of Excellence, 2008, Analysis of the 2007 Cyber Attacks against Estonia from the Inf (ccdcoe.org); CZOSSECK C., OTTIS R., TALIHÄRM A.-M., *Estonia after the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security,* in «*International Journal of Cyber Warfare and Terrorism (IJCWT)*», Vol.1(1), 2011, pp. 24–34.

16 NATO - Official text: Warsaw Summit Communiqué issued by NATO Heads of State and Government (2016), 09-Jul.-2016.

17 *The North Atlantic Treaty, Washington DC*, April 4, 1949, NATO - Official text: The North Atlantic Treaty, 04-Apr.-1949.

18 NATO - Official text: Brussels Summit Communiqué issued by NATO Heads of State and Government (2021), 14-Jun.-2021.

19 NATO - Official text: Vilnius Summit Communiqué issued by NATO Heads of State and Government (2023), 11-Jul.-2023.

20 NATO - Official text: London Declaration issued by NATO Heads of State and Government (2019), 04-Dec.-2019.

21 See *supra* note DA VEDERE

22 Following the NATO Vilnius Summit in July 2023, allies are developing a commercial space strategy to accelerate military technologies. Based on recommendations from a NATO-industry working group, the strategy aims to leverage commercial space capabilities, improve space situational awareness, and streamline acquisition processes to enhance defense cooperation and security in space. Source: HITCHEN T., *NATO plans first commercial space strategy to spur tech innovation*, Breaking Defence, 2024, NATO plans first commercial space strategy to spur tech innovation - Breaking Defense.

23 *Integrating Commercial Space for Military Applications in Europe: A Challenge and Opportunity*, ESPI, 2024 (para. 5) Integrating Commercial Space for Military Applications in Europe: A Challenge and Opportunity - ESPI.

24 NATO - Official text: Madrid Summit Declaration issued by NATO Heads of State and Government (2022), 29-Jun.-2022.

25 MARTINO L., *Cyber e Spazio: nuovo fronte di difesa integrata*, ISPI, 2022, Cyber e Spazio: nuovo fronte di difesa integrata | ISPI (ispionline.it).

managing the chain of command and control, identifying targets, guiding drones or weapons, and performing numerous other military activities[26].
In addition to the efforts of NATO member States, other initiatives are also worth mentioning: the *European Cybersecurity Skills Framework* (ECSF) developed by ENISA in 2022[27], the *NIST Cybersecurity Framework*, created by the U.S. National Institute of Standards and Technology (NIST)[28] and the *PANDORA-EDIDP Project* an EU-funded cyber defense platform designed for real-time threat hunting, incident response, and information sharing[29]. At this stage of the analysis, it is evident that space assets are crucial for delivering services to both military and civilian sectors. However, the growing interconnection between those two domains has significantly increased the vulnerability of space systems to cyber threats. While cyberattacks discussed in the introduction may not meet the threshold of an "armed attack" under *jus contra bellum*, their disruptive impact raises pressing questions about the capacity of International Law to address these emerging challenges effectively. Specifically, which principles of International Law can effectively prevent and address cyberattacks targeting space systems, particularly the ground segment? The following section examines the principle of due diligence, evaluating its potential as a regulatory framework while critically underling its limitations.

2. The principle of due diligence in International Law

According to Professor Ian Yuying Liu, due diligence is a corollary of State sovereignty[30]. This obligation is not a rule of attribution, but a primary norm derived from the judgment of the International Court of Justice (ICJ) in the *Corfu Channel Case* and, more recently, in *Pulp Mills Case*[31]. Briefly examining the two cases, the

---

[26] To know more about the use of space technologies in the military sector see: NATO Science & Technology Organization. *Science & Technology Trends 2023-2043: Across the Physical, Biological, and Information Domains*. Volume 2: Analysis, 2023, pp. 164-178.

[27] ECSF is a tool aimed at harmonizing cybersecurity education and workforce development across Europe. It defines roles and skills necessary for cybersecurity professionals, helping bridge the gap between the supply (training) and demand (workplace) sides in the EU cybersecurity workforce. Source: European Cybersecurity Skills Framework (ECSF) — ENISA (europa.eu).

[28] The framework provides a set of guidelines to help organizations manage and reduce cybersecurity risks. It is widely adopted globally and structured around five core functions: Identify, Protect, Detect, Respond, and Recover. Source: Cybersecurity Skills and Workforce Frameworks | NIST.

[29] Financed by the European Commission under the European Defence Industrial Development Programme (EDIDP), PANDORA supports collaborative cyber defense among EU member states. The project focuses on strengthening cyber resilience within the EU by providing innovative tools and solutions for better threat management and incident handling. Source: PANDORA-EDIDP.

[30] LIU Y.I., *State Responsibility and Cyberattacks: Defining Due Diligence Obligations*, in «The Indonesian Journal of International and Comparative Law», 2017, p. 199.

[31] As affirmed by Doctor Jack Kenny, due diligence obligations have been addressed in a number of international courts and arbitral awards…See: International Court of Justice, Corfu Channel Case (United Kingdom v. Albania), 9 April 1949, I.C.J. Reports 1949, p. 4, p. 22; International Court of Justice, Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), 26 February 2007, I.C.J. Reports 2007, p. 43, para. 430; International Court of Justice, Pulp Mills on the River Uruguay (Argentina v. Uruguay), 20 April 2010, I.C.J. Reports 2010, p. 14, paras 101, 197, 204, 223; International Court of Justice, Certain Activities Carried Out by Nicaragua in the Border Area (Costa Rica v. Nicaragua) and Construction of a Road in Costa Rica along the San Juan River (Nicaragua v. Costa Rica), 16 December 2015, I.C.J. Reports 2015, p. 665, paras 104, 153, 168, 228; International Tribunal for the Law of the Sea, Responsibilities and Obligations of States Sponsoring Persons and Entities with Respect to Activities in the Area (Advisory Opinion), 1 February 2011, ITLOS Reports 2011, paras 110–112, 117–120, 131–132; International Tribunal for the Law of the Sea, Request for an Advisory Opinion Submitted by the Sub-Regional Fisheries Commission, 2 April 2015, ITLOS Reports 2015, paras 125–132, 146–150.

former concerned a dispute between the United Kingdom and Albania centred on an incident that occurred on 22 October 1946. During that time, two British warships struck mines and sustained significant damage while navigating the Corfu Channel within Albanian territorial waters. The Court held Albania responsible under International Law for the explosions and the resulting casualties and damage. It concluded that Albania's responsibility was due to its failure to inform the United Kingdom about the presence of mines in its waters. The Court based this duty to notify on "certain general and well-recognized principles", which include «[E]very State"s obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States»[32].

In the more recent *Pulp Mills Case*, the issue presented to the Court concerned Uruguay's responsibility for breaching environmental obligations under a 1975 bilateral Treaty with Argentina[33]. To determine the scope of Uruguay's obligations under this Treaty, particularly regarding the preservation and protection of the San Juan River ecosystem, the Court referred to the customary obligation to prevent transboundary environmental harm, noting: «[T]he principle of prevention, as a customary rule, has its origins in the due diligence that is required of a State in its territory»[34]. Although the status of the no-harm rule was uncertain at the time of the judgment, it is now established that States have a customary International Law obligation to prevent their territory from being knowingly used for actions that violate the rights of other States[35].

Analysing some doctrinal interpretation of the due diligence principle in International Law, it is possible identify contrasting positions. Indeed, as McDonald explains, «there is no "general principle of due diligence" in International Law, a legal requirement to exercise due diligence may be a component part of a primary rule of International Law, but this can only be determined by referring back to the primary rule in question»[36]. Moreover, in relation to the *Corfu Channel* case, McDonald asserts that the Court did not identify a universal source for a general obligation of due diligence, nor did it extend due diligence obligations developed in specific contexts to other areas as if they were universally applicable[37]. In contrast, according to Koivurova, many areas of International Law have developed primary obligations that require States to exercise due diligence. These obligations do not require States to achieve a specific outcome but rather to make efforts to reach the result set out in the obligation[38]. In addition, a research elaborated by *Max Planck Institute for Comparative Public Law and International Law* suggested that due diligence may operate as a primary obligation in various fields, requiring States to take measures to mitigate risks, including those posed by non-state actors[39].

---

32 International Court of Justice, *Corfu Channel* (United Kingdom of Great Britain and Northern Ireland v. Albania), April 9, 1949, ICJ Reports 1949, p. 22.

33 *Statute of the River Uruguay*, a treaty signed by the two States on 26 February 1975, available at the following: Uruguay_River_Statute_1975.pdf (internationalwaterlaw.org)

34 International Court of Justice, *Pulp Mills on the River Uruguay* (Argentina v. Uruguay), 20 April 2010, I.C.J. Reports 2010, p. 14, para. 101.

35 OLLINO A. *Due Diligence Obligations in International Law*, Cambridge University Press: Cambridge, United Kingdom, 2022, p. 54.

36 MCDONALD N., *The Role of Due Diligence in International Law,* in «Cambridge University Press» (2016) p. 1041.

37 OLLINO A. *Due* ...op. cit. pp. 54-57; KENNY J. *A general obligation of due diligence in international law*?, European Journal of International Law, 2024.

38 KOIVUROVA T., *Due Diligence*, in R Wolfrum (ed), *Max Planck Encyclopedia of Public International Law*, 2010.

39 *Ibidem*.

Moreover, as affirmed by Professor Karine Bannelier-Christakis: «[T]oday, everybody agrees that the *dictum* of the Court expresses a general principle of International Law». In this regard, it is important to clarify that the aim of this paper is not to extrapolate the concept of due diligence from other fields of International Law to determine whether it constitutes a general principle of International Law. Instead, the focus is on understanding the specific characteristics of the obligation under discussion and exploring its application in the context of cyberattacks.
As expressed by many scholars, due diligence is an obligation of conduct and not of a result[40]. According to S. Heathcote: «[S]tates should "deploy their best efforts to achieve [the] desired outcome[…]even if that outcome need not be ensured»[41]. To better understand the difference between a norm of conduct compared to a norm of result it is useful cite the ICJ pronunciation in the Genocide Case: «[I]t is clear that the obligation in question is one of conduct and not one of result, in the sense that a State cannot be under an obligation to succeed, whatever the circumstances, in preventing the commission of genocide: the obligation of States parties is rather to employ all means reasonably available to them, so as to prevent genocide so far as possible. A State does not incur responsibility simply because the desired result is not achieved; responsibility is however incurred if the State manifestly failed to take all measures to prevent genocide which were within its power, and which might have contributed to preventing the genocide. In this area the notion of "due diligence", which calls for an assessment *in concreto*, is of critical importance»[42].
Having gained a clearer understanding of the origins and primary characteristics of due diligence in International Law, it is now essential to assess its potential application in the context of cyberspace.

2.1. Due diligence in cyberspace

According to the examination of the Court judgments, it is evident that the obligation is strictly related to the concept of territorial sovereignty, as a consequence, to apply it in cyberspace it is important to clarify if the cyber domain can be considered as a territory under the sovereignty of a State. To answer this question, some academics have affirmed that «[c]yberspace, as an intangible medium, can only exist inside tangible infrastructure […]. It operates via networks of computers, information systems, and telecommunication infrastructures located within a State's territory»[43]. Moreover, based on the interpretation of certain scholars who consider due diligence a general principle of International Law, as derived from ICJ judgments, this principle can consequently be extended to all activities, including those occurred in

---

40 "It is an obligation of conduct, not an obligation of result" stated the International Law Commission in its commentary of Article 7 concerning the due diligence that watercourse States need to exercise. International Law Commission, 'Draft Articles on the Law of the Non-Navigational Uses of International Watercourse sand Commentaries thereto and Resolution on Transboundary Confined Groundwater', Report of the International Law Commission on the Work of its Forty-sixth Session, 1994. In a similar way see also Pulp Mills, supra note 7, paras. 186–187.

41 HEATHCOTE S., *State Omissions and Due Diligence: Aspects of Fault, Damage and Contribution to Injury in the Law of State Responsibility*, in Bannelier K. - Christakis T. - Heathcote S. (eds.), *The ICJ and the Evolution of International Law: The Enduring Impact of the Corfu Channel Case*, London-New York, Routledge, 2012, p. 308.

42 International Court of Justice, *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*, February 26, 2007, ICJ Reports 2007, para. 430.

43 WINGFIELD T., *The Law of Information Conflict*, U.S. Dep't. of Defense, Dictionary of Military and Associated Terms, 2000.

cyberspace[44]. At the international level, part of the community promotes application of the due diligence principle in cyberspace. Indeed, its legitimate application is cited in Rule13c[45] of the Report of the Group of Governmental Experts (GGE) *On Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*[46] and in Rule number 5[47] of the *Tallinn Manual 1.0*[48]. Rule 13c establishes that «States should not knowingly allow their territory to be used for internationally wrongful acts using Information-Communication-Technologies (ICTs)»[49]. While Rule 5 of the *Tallinn Manual* affirms «a State must exercise due diligence in not allowing its territory, or territory or cyber infrastructure under its governmental control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences for, other States»[50].

Many State practices can be referenced to suggest that the due diligence principle could be applicable in cyberspace. One relevant example is the *American International Strategy for Cyberspace*, which includes due diligence in cybersecurity as a new and essential emerging norm in this context, defining it as: «the responsibility of States to protect information infrastructures and secure national systems from damage or misuse». Similarly, Italy asserts that the obligation of due diligence applies to cyberspace. Consequently, it requires States to adopt all reasonable measures concerning activities conducted within cyberspace under their jurisdiction, to prevent, eliminate, or mitigate potentially significant harm to the legally protected interests of another State or the international community. Furthermore, Italy maintains that due diligence is an obligation of conduct, not of

---

44 BANNELIER-CHRISTAKIS K., *Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations?*, in «Baltic Yearbook of International Law»,14(2014), p. 5.

45 UN Doc A/76/135, July 14, 2021.

46 The constitution of Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security was established by United Nations General Assembly Resolution 73/266. The Group of Experts comprises 25 members representing major UN Member States. The primary goal of the Report, and the ongoing analytical work by the GGE, is to promote "a common understanding and effective implementation of potential cooperative measures to address existing and potential threats in the realm of information security." Although the norms on Responsible State Behaviour are not legally binding, their development reflects a consensus of thoughts and practices supported by numerous states, which in turn fosters the creation of binding customary practices.

47 SCHMITT M., NATO Cooperative Cyber Defence Centre of Excellence, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge: Cambridge UP, 2013. p. 26.

48 To facilitate the application of international law to the cyber context, the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), inspired by the San Remo Manual on International Law Applicable to Armed Conflicts at Sea, established a Governmental Group of Experts (GGE) to draft a manual aimed at assisting in the application of jus ad bellum and jus in bello in the context of cyber warfare. As a result of this initiative, the Tallinn Manual on the International Law Applicable to Cyber Warfare 1.0 and 2.0 was produced, with the most recent edition published in 2017. However, some academics and non-Western states such as China and Russia have raised concerns regarding the drafting of the aforementioned Manual. The primary criticisms focus on the composition of the Group of Experts, which is perceived to be overly representative of a "Western" perspective; nine out of the 23 members were American, while none were from countries like Russia, China, Iran, or Israel. Additionally, there is insufficient analysis of the principle of non-intervention, and the threshold at which a cyber operation can be considered “use of force” has not been definitively established. Moreover, the criteria for attribution are also not thoroughly discussed. Sources: SCHMITT M., *NATO Cooperative Cyber Defence Centre of Excellence, Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge: Cambridge UP, 2013; FLECK D., *Searching for International Rules Applicable to Cyber Warfare—A Critical First Assessment of the New Tallinn Manua*l, in «Journal of Conflict and Security Law», 2013, pp. 331-335.

49 Vedi *supra* note 44 p. 10.

50 Vedi *supra* note 46.

result. Therefore, a State that demonstrates its commitment to halting or limiting the execution of illicit cyber activities initiated from or transiting through its territory cannot be held responsible for failing to achieve these goals (cessation or limitation of the illicit activity)[51]. In addition to these three examples, statements from other States can be used to support the opinion that due diligence constitutes a general international obligation for every State not to knowingly allow its territory to be used for internationally wrongful acts involving cyber means. Some of the States that have adopted this approach are: Australia[52], Czech Republic[53], Estonia[54], France[55], Germany[56], Japan[57], the Netherlands[58], Norway[59], Switzerland[60], and Sweden[61].

To conclude the evaluation of the due diligence application in cyberspace, deserved to be mention the position expressed by the Council of the European Union in its *Declaration on a Common Understanding of International Law in Cyberspace*, approved on November 2024. In the annex, and more precisely at its point 3, it is asserted as follows: «Due diligence is a principle of International Law that applies in the cyber context […]. As States have jurisdiction over ICT infrastructure and individuals as referred to in Section 1 above[62], they are required to make efforts that this ICT infrastructure is not used by non-state or State actors for acts contrary to the rights of other States, once they know or ought to have known of such activities. States are required to take all appropriate and reasonably available and feasible measures […] to act against cyber operations that violate rights of another State under International Law. The same duty applies for cyber activities within the territory or ICT infrastructure that they otherwise effectively control»[63].

Having established the origins of the obligation and its hypothetical application in cyberspace, it could be argued that a State's failure to exercise due diligence commit an internationally wrongful act. At the same time, invoking the international responsibility regime for such acts would require determining when a State is considered to have violated the due diligence obligation in the context of cyberspace activities. To do so, is essential referring to the text of the provision and, specifically, to the Rule13c of the GGE Report[64], which best represent the opinion of the international community concerning due diligence application in cyberspace. Reading the text of Rule 13c, it is certain that to invoke international responsibility is first necessary demonstrate that the State from whose territory the cyberattack is

---

51 *Italian Position Paper on International Law and Cyberspace*, 2021, pp. 6-7, italian_position_paper_on_international_law_and_cyberspace.pdf (esteri.it)

52 Australia's International Cyber Engagement Strategy (dfat.gov.au)

53 czech-republic-oewg-pre-draft-suggestions.pdf (un-arm.org)

54 president.ee

55 National position of France (2019) - International cyber law: interactive toolkit

56 on-the-application-of-international-law-in-cyberspace-data.pdf (auswaertiges-amt.de)

57 100200935.pdf (mofa.go.jp)

58 Letter to the parliament on the international legal order in cyberspace | Parliamentary document | Government.nl[59]

59 A-76-136-EN.pdf (un-arm.org)

60 Switzerland's Position Paper on the Application of International Law in Cyberspace • Page 1 • UNIDIR Cyber Policy Portal Database

61 Sidan kan inte hittas - Regeringen.se

62 Section 1 of the Council of the European Union, *Declaration on a Common Understanding of International Law in Cyberspace*, 18 November 2024, Brussels, Press Release No. 1234/24, reads as follow: States exercise territorial jurisdiction over Information and Communications Technology (ICT) infrastructure located in their territory, and persons engaged in cyber activities, within their territory.

63 *Ibidem*.

64 Vedi *supra* note 48.

carried out must be aware about that. Such knowledge can be considered constructive if, under normal circumstances, the State would or should have been aware of the harm coming from its territory or infrastructures under its control and jurisdiction. The concept of constructive knowledge related to due diligence in cyberspace, is well supported by several States, such as Finland, Northway, Romania and Switzerland[65]. However, this perspective does not obligate a State to implement preventive measures with its cyber infrastructure, nor does it require the State to monitor all its infrastructure to stay informed about potential transboundary harm[66]. Indeed, States can interdict a cyberattack only if they are aware about that but, in cyberspace, the time between an attack initiation and conclusion is very limited and the real origin of a cyberattack can be falsified. Indeed, it is easy for both State and non-state actors falsifying the true origin of attacks, using, for example, a simple VPN[67]. Moreover, States frequently use proxies to conduct cyber activities with the intent of denying attribution[68]. To solve this problem, and not incur in a false attribution, the applicant must provide solid, unbiased evidence showing the respondent should have known about the cyberattack. This may include expert testimony on network logs or documentary evidence like press reports. An international tribunal can also appoint its own experts to verify the reliability of such evidence[69].

The second aspect to verify is if the cyberattack is contrary to the rights of another State. Only cyberattacks of a certain level of gravity will engage a State's due diligence obligation. Indeed, the obligation deals with only cyberattacks that amount to an internationally wrongful act[70] and which result in serious adverse consequences for the target State. Under the laws of state responsibility, harm is not a prerequisite for identifying an internationally wrongful act. However, in cases involving due diligence, the existence of damage is essential to confirm a breach of the primary rule[71]. To understand when the "serious injury" trigger the due diligence obligation in cyberspace, could be useful mentioning the definition of "unlawful cyber act" provided in the *Tallin Manual 1.0*. Accordingly, an "unlawful [cyber] act" is defined as any cyber activity originating from one State"s territory that impacts the rights of other States, resulting in a negative outcome[72]. To better understand the level of harm required to trigger the due diligence obligation in cyberspace, it is useful to analyse the various definitions provided by relevant academics and international documents. For instance, the *Tallinn Manual* 1.0 suggests that physical damage to objects or harm to individuals is not always necessary to classify a cyberattack as unlawful[73]. The notion of "serious injury" is assessed retrospectively and does not dictate what actions a State should take during

65 KASTELIC A., *Due diligence in cyberspace …*p.13.

66 TALBOT JENSEN E., *The Tallinn Manual 2.0: Highlights and Insights*, in «Georgetown Journal of International Law 735», Vol. 48 (2017), p. 745.

67 VPN: Virtual Private Network, a virtual private network that ensures privacy, anonymity, and security through a dedicated communication channel created over a public network infrastructure. Source: LOMBARDO S., *VPN: cos'è, come funziona e per cosa viene utilizzata una rete privata virtuale*, Cybersecurity 360, 2022, VPN, cos'è la Virtual Private Network e quali sono i vantaggi (cybersecurity360.it)

68 TALBOT JENSEN E., *The Tallinn Manual 2.0: …,* op. cit., pp. 745-746.

69 LIU Y.I., *State Responsibility …*op. cit., pp. 239-240.

70 Draft articles on Responsibility of States for Internationally Wrongful Acts (ARISWA), 2021, Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries - 2001 (un.org)

71 LIU Y.I., *State Responsibility …*op. cit., pp. 242.

72 SCHMITT M., NATO Cooperative Cyber Defence Centre of Excellence, *Tallinn Manual …*op. cit., p. 26.

73 *Ibidem* (Rule 1 and 5).

the attack itself. To support this view, reference can be made to Professor Roscini's definition of cyberattacks, where he noted that those causing physical damage comparable to conventional attacks could amount to the use of force or an armed attack. He also affirmed that cyberattacks targeting National Critical Infrastructure[74] could also meet the threshold of the use of force[75]. In the hypothetical event of a cyber-attack causing this level of damage, the State that suffers the damage is more likely to invoke a violation of Article 2(4) of the UN Charter[76] or the right of self-defence enshrined in article 51 of the UN Charter[77], rather than focusing on the due diligence obligation. Consequently, this high threshold of injury is inappropriate for triggering due diligence in cyberspace, instead, a lower level of damage should also be sufficient to activate (cyber) due diligence. According to the paper elaborated by Professor Liu, a cyberattack is considered "destructive" and results in "serious injury" once it causes significant disruptions to a network's functionality. Due diligence obligations should be triggered as soon as the initial injury incapacitates the network, reaching the threshold of "destructiveness"[78]. To determine whether a cyberattack is "destructive", a relevant and useful definition is the one elaborated in the *Budapest Convention on Cybercrime*[79], which defines system interference as «the serious hindering […] of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data». Considering the network interdependency, cyberattacks could cause consequent harm to society without physical damages. As a consequence, cyberattacks which provoke temporary or permanently loss of network's functionality that provide essential services, like transport, healthcare, communications etc. can trigger due diligence obligation.

For a complete analysis of the concept of "serious injury", it is also important to consider the types of cyberattacks that are deemed to have an insufficient level of injury to trigger the obligation. One of this category is represented by cyber exploitation activities, which are defined as an "unauthorized access to computers, computer systems, or networks, in order to exfiltrate information, but without affecting the functionality of the accessed system or amending/deleting the data

---

74 Vedi *supra* note 1.

75 ROSCINI M*., Cyber Operations and the Use of Force in International Law*, Oxford: Oxford University Press, 2014, pp.52-58.

76 Article 2 (4) of the UN Charter reads as follows: «All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations». *Charter Of The United Nations And Statute Of The International Court Of Justice*, San Francisco 1945, https://treaties.un.org/doc/Publication/CTC/uncharter.pdf

77 Article 51 of the UN Charter reads as follows: « Nothing in the present Charter shall impair the inherent right of individual or collective self defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken the measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self defense shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security». *Charter Of The United Nations And Statute Of The International Court Of Justice*, San Francisco 1945, https://treaties.un.org/doc/Publication/CTC/uncharter.pdf

78 LIU Y.I., *State Responsibility …*op. cit., pp. 248.

79 The Budapest Convention on Cybercrime, also known as the Council of Europe Convention on Cybercrime, is the first international treaty designed to address internet and computer crimes by harmonizing national laws, improving investigative techniques, and increasing cooperation between countries. Adopted in 2001, it remains a key instrument for combating cybercrime globally. Too know more about the Budapest Convention see: Budapest Convention - Cybercrime (coe.int).

resident therein"[80]. For the purposes of this paper, since cyber exploitation does not cause a loss of functionality or physical injury, it cannot be classified as a cyberattack that would trigger the due diligence obligation. In addition to the two elements, another requirement needs to be fulfilled to invoke due diligence obligation violation, namely, the "feasibility measures". The "feasibility" of measures for a State will depend on the technical and financial resources at its disposal. Indeed, a State will not breach International Law if it does not successfully end or prevent a cyberattack stemming from its territory which is too complex to be controlled by its capabilities. Furthermore, even in instances where States have the capacity to prevent harmful cyber operations carried out in their territory, they are under no obligation to do so when it would be unreasonable in the circumstances (denial its essential services to hamper the attack). To better understand the types of measures required, it is helpful to examine the non-exhaustive list provided in Rule 13C of the GGE Report. Some of them include: (a) States are expected to take reasonable, proportionate, and effective steps within their capacity to end ongoing activities in their territory, consistent with international and domestic law, although it is not expected that States monitor all ICTs activities within their territory; (b) States aware of, but unable to, address wrongful ICTs acts within their territory may seek assistance from other States or the private sector, adhering to international and domestic laws. Establishing structures for assistance requests can aid implementation. States should act in good faith and not exploit the situation for malicious activities against the requesting State or third States; (c) An affected State should notify the State from which the activity originates. The notified State should acknowledge receipt to facilitate cooperation and make efforts to determine if a wrongful act occurred. Acknowledgement does not indicate agreement with the notification[81].

Having concluded the analysis of the due diligence obligation, it can now be argued that it is possible to apply this obligation in cyberspace. However, as of today, its application still depends on the willingness of States. Moreover, the difficulty in applying and invoking it in the event of a possible violation is objectively significant. The primary critical concern pertains to the unique characteristics of cyberspace, which render more difficult identify the origin of the attacks and consequently attribute the conduct to a State. A clearer definition of the legal characteristics of the due diligence obligation in relation to cyberspace could certainly promote its application, thereby reducing the number of potential cyberattacks, regardless of whom they are directed against. In this sense, it could be interesting to better define the obligations derived from this provision, such as the list indicated in Rule 13c. What is encouraging is the expanding State practice supporting the application of the due diligence principle in cyberspace. A prominent example of this tendency is represented by the Council of the European Union Declaration, which may pave the way for similar approaches by other States.

To further elaborate on this topic, the ViaSat case study serves as an illustrative example that allows for an examination of the application of the due diligence principle in cyberspace, particularly in relation to cyberattacks targeting the ground segment of space systems.

[80] ROSCINI M., *Cyber operations* …op. cit., p.17.
[81] UN Doc A/76/135, 2021, p. 10.

3. ViaSat cyberattack and the application of the due diligence

3.1. Technical characteristics of ViaSat cyberattack

Prior to examining the general characteristics of the cyberattack in question, it is essential to clarify the rationale for specifically applying the due diligence principle to cyberattacks targeting the ground segment. Firstly, cyberattacks are more likely to exploit vulnerabilities in the ground segment, making it a critical focal point for such analysis. Moreover, a comprehensive legal examination of cyberattacks directed at the link or space segments of a space system would also require addressing the application of the due diligence principle in the outer space domain, a topic that would necessitate an entirely separate and extensive study.

Having clarified this, it is appropriate to dedicate some attention to the characteristics of the ground segment of a space asset. The ground segment is essential for communication between satellites and user terminals, encompassing infrastructure such as gateway stations, control systems, and network management facilities like the Network Control Centre (NCC) and the Network Management Centre (NMC), which manage satellite access requests. It also includes earth terminals and user receivers that transform satellite signals into usable data for devices such as modems, antennas, and mobile phones[82]. Command and control systems ensure satellite functionality, and for LEO constellations, numerous globally distributed ground stations are required to maintain communication[83].

The ground segment value chain comprises interconnected processes and stakeholders involved in operating satellite communication infrastructure. It is divided into three blocks: a) Upstream: Includes hardware and software for operations, such as antennas and modems, along with launch facilities and networks connecting ground segment components; b) Midstream: Covers mission support activities like satellite control, signal downlinking, and data retrieval; c) Downstream: Focuses on data processing, storage, and analytics-based services after reception. This segmentation ensures efficient and reliable satellite communication system operations[84].

Having provided some general notions about the function and structure of the ground segment, it is now time to shift attention to the ViaSat cyberattack. On February 24, 2022, Viasat"s KA-SAT network suffered a major disruption caused by a malware-based wiper attack that rendered thousands of end-user terminals inoperative[85]. As clarified by ViaSat in a subsequent press release, the attack specifically targeted a "consumer-oriented partition" of the KA-SAT network, including Tooway, SurfBeam2, and SurfBeam2+ Internet modems, rather than the satellite itself[86]. The consequences of the attack were widespread, affecting users not only in Ukraine but across Europe.

In Ukraine, the attack impacted key users such as the government, military, and security services. The disruption extended beyond Ukrainian borders, affecting

---

82 CASARIL F. - GALLETTA L., *Securing SATCOM user segment: A study on cybersecurity challenges in view of IRIS,* in «Computers & Security» 140 (2024), p. 3. http://dx.doi.org/10.1016/j.cose.2024.103799.

83 PwC, 2020. Market perspectives of ground segment as a service (gsaas).

84 *Ibidem*.

85 Viasat News Blog, 2022. Ka-Sat network cyber-attack overview. KA-SAT Network cyber attack overview - Viasat.

86 *Ibidem*.

around 9,000 users of the French NordNet satellite broadband service[87] and nearly 15,000 customers of BigBlu, a British provider, across Germany, France, Hungary, Greece, Italy, and Poland[88]. Enercon, a German energy company, also experienced operational setbacks, losing remote monitoring and control over its 5,800 wind turbines due to their reliance on the KA-SAT network"s SCADA system[89].
Interestingly, the segment of the network targeted in the attack is owned by ViaSat, a U.S.-based company, but operated by Skylogic, a subsidiary of Eutelsat. The attack unfolded in two distinct stages[90]: a) Denial-of-Service Attack: exploiting vulnerabilities in the authentication mechanisms of Viasat modems, particularly in Ukraine and Germany, to gain unauthorized access to the ground and user segments. This caused a service outage that took several days to fully resolve; b) Network Infiltration: leveraging a separate vulnerability in Skylogic"s VPN appliances to breach the ground network management segment. The attackers moved laterally within the network, disrupting communications for over 15,000 users, including governmental and military entities.
The case study clearly demonstrates the direct interconnection between space and cyberspace, highlighting the critical vulnerabilities that permeate satellite communication systems with respect to cyberspace. It is now possible to try to attribute to the Russian Federation the violation of the due diligence obligation.

3.2. Attempt to attribute to the Russian Federation the breach of the due diligence obligation in relation to ViaSat cyberattack

Before evaluating the alleged violation of the due diligence obligation by the Russian Federation, it is important to examine the international response to the wrongful act in question. A few months after the cyberattack on satellite communication networks, the United States[91], the United Kingdom[92], and the European Union[93] publicly attributed responsibility for the attack to the Russian Federation. The first authority to hold Russia accountable for the February 24 cyberattack was the European Union's High Representative, Josep Borrell, followed by representatives from the United States, the United Kingdom, Canada, and Estonia[94]. Additionally, the United Kingdom's National Cyber Security Centre (NCSC) declared it was "almost certain" that Russia was behind the attack[95]. Furthermore, some U.S. officials claimed that Russian military hackers were responsible for the cyberattack on the satellite service. However, Saloni Sharma,

87 ConnexionFrance, 2022. Thousands in France lose Internet in suspected Russian cyberat tack. Thousands in France lose internet in suspected Russian cyberattack.
88 Techq, 2022. Thousands of Internet users go dark in Europe from 'cyberattack'. Technology News | TechHQ | Latest Technology News & Analysis.
89 ENERCON, 2022. Over 95following disruption to satellite communication. Enercon turbines disrupted by satellite cyber attack - Modern Power Systems.
90 Reversemode, 2022. VIASAT incident: from speculation to technical details. VIASAT incident: from speculation to technical details.
91 BIEIESEKER C., *US and EU Officials Attribute Viasat Cyber Attack to Russia*, Via Satellite, 2022, US and EU Officials Attribute Viasat Cyber Attack to Russia - Via Satellite (satellitetoday.com)
92 VILLANCE C., *UK blames Russia for satellite internet hack at start of war*, BBC News, 2022, UK blames Russia for satellite internet hack at start of war (bbc.com).
93 BIEIESEKER C., *US and EU Officials Attribute* …op. cit.
94 Council of the EU. (May 10, 2022). Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union [Press release], Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union - Consilium (europa.eu)
95 VILLANCE C., *UK blames Russia for satellite* … op. cit.

spokesperson for the National Security Council, stated: «At this time, we have no attribution to share and are closely examining the issue»[96]. When asked about the responsibility for the cyberattack, Victor Zhora, Deputy Chief of the State Service of Special Communications and Information Protection, Ukraine's main Cybersecurity Agency, responded: «We do not need to attribute it as we have clear evidence that it was organized by Russian hackers to disrupt the connection among customers using this satellite system»[97]. It worths mentioning that after the cyberattacks, Russia fell victim to a hacking operation that resulted in the loss of control over two of its satellites. The Russian Space Research Agency (ROSCOSMOS) commented on this incident, stating: «A cyber operation that caused the loss of contact between its reconnaissance satellites and the ground station is considered an act of war»[98].

In order to understand whether Russia has breached its due diligence obligation, it would be preferable to use as a reference the GGE Report *On Advancing Responsible State Behaviour in Cyberspace in the Context of International Security* rather than the *Tallinn Manual 1.0 or 2.0*. This preference is due to the fact that, first of all, a representative of the Russian Federation is a member of the GGE and secondly, the *Tallinn Manual*s represent a minority of States within the international community while the GGE Report involves many countries located all over the world.

Reporting on Rule 13c: «States should not knowingly allow their territory to be used for international wrongful acts using ICTs»[99]. As better explained in section 2.1, the provision implies that if a State is aware of or is notified in good faith that an internationally wrongful act, conducted with the assistance of ICTs, originates from or transits through its territory, it must take all appropriate and reasonably available and feasible measures to identify and address the situation. Furthermore, Rule 13c prohibits a State from allowing another State or a non-state actor to use ICTs within its territory to commit internationally wrongful acts[100].

In the context of the ViaSat case study, assessing whether the Federation breached its due diligence obligation involves examining whether Russia, upon being aware of the wrongful act originating from or transiting through its territory, took all necessary measures to address the situation. Regarding knowledge of the wrongful act, it is undeniable that Russia was aware of the cyberattack targeting the Ka-Sat network. This assertion is supported by the fact that the cyberattack occurred just hours before the actual invasion by Russian troops into Ukrainian territory. This timing provided a significant advantage to Russian forces by "blinding" the Ukrainian command and control chain. Therefore, it is highly probable that the wrongful act was perpetrated by Russian intelligence services or, alternatively, organized and planned by Russia itself, thus making it fully aware of the cyberattack.

One aspect that remains impossible to verify is the exact origin of the malicious operation, which, in cyberspace, is among the most challenging elements to ascertain. Understanding this would help determine whether the act was carried out

---

96 NAKASHIMA E., *Russian military behind hack of satellite communication devices in Ukraine at war's outset, say*, The Washington Post, 2022, Russian military behind hack of satellite communication devices in Ukraine at war's outset, U.S. officials say - The Washington Post.

97 *Ibidem*.

98 VÄLJATAGA A., *Cyber vigilantism in support of Ukraine: a legal analysis*, CCDCOE, 2022, p. 3.

99 Vedi *supra* note 48.

100 Vedi *supra* subsection 2.1.

within or outside Russian territory and consequently, ascertain whether it constitutes a cyberattack "transiting or originating" from the Federation, in order to establish a violation of (cyber) due diligence. In the case at hand, assuming the attack was indeed perpetrated by the GRU[101], an entity known to utilize the information technology infrastructure of the Federation's Armed Forces along with their developed information and communication technologies for its cyber activities, it becomes highly probable that the attack originated within the Federation's territory. Given this hypothetical scenario, it can be confidently stated that not only was the Russian Federation fully aware of the wrongful act, but also that it originated from its own territory, thereby fulfilling the criteria outlined by the obligation under examination.

The second element to assess is whether the cyberattacks caused a "serious injury" to the affected State, thereby violating its rights. As discussed in subsection 2.1, a "serious injury" in cyberspace is typically considered to occur when a cyberattack results in the temporary or permanent loss of functionality of networks that provide essential services, such as transportation, healthcare, or communications etc. In this specific scenario, the loss of network functionality is undeniably evident. The ViaSat cyberattack not only disrupted the chain of command and control for Ukrainian troops but also severely impaired the communications of Ukrainian citizens and the government. Furthermore, the attack's effects extended beyond Ukraine's borders, as highlighted in section 3.1. States such as Germany, the United Kingdom, Italy, Poland and France experienced some of the repercussions. Consequently, it is reasonable to conclude that the "serious injury" criterion is fully satisfied in this case study, given the widespread and significant impact of the cyberattack.

Once it is established that the State in question was aware of the wrongful act, that it originated from its territory, and that the attack caused a "serious injury" to the affected State, a breach of the due diligence obligation can be demonstrated by showing that the Federation failed to take the actions required by this obligation. Despite the obligations have been already mentioned in subsection number 2.1, reporting it would be useful to better apply the provision in this peculiar case study. Again, some of the obligations are: a) States must take appropriate steps to stop activities within their territory, but are not required to monitor all ICTs activities; b) If a State cannot address wrongful ICTs acts, it can seek help from other States or the private sector, following laws. Establishing assistance structures can aid implementation. States should act in good faith and avoid exploiting the situation maliciously; c) An affected State should notify the State of origin of the activity, which should acknowledge receipt and cooperate to determine if a wrongful act occurred. Acknowledgment doesn't imply agreement with the notification etc[102].

At present, there is no evidence that the Russian Federation has taken steps to address the damage caused by the attack. If the hypothesized scenario were confirmed—namely, that Russia was aware of the attack's origin within its territory—it could be argued that the Federation failed to fulfil its duty to prevent, counter, or terminate the malicious activity. This would constitute a clear violation of its due diligence obligations. Furthermore, Russia's prominent capabilities in the field of information technology make it difficult to argue that a failure to act could

[101] GRU stands for Main Intelligence Directorate - outlasted the KGB when the Soviet Union collapsed in 1991 and appears to be flourishing today. To know more consult the following link: Why Russia's GRU military intelligence service is so feared (bbc.com)

[102] Vedi *supra* note 80.

be attributed to a lack of capacity. Even if Russia was, hypothetically, unable to mitigate the ongoing damage due to capacity limitations, the principle of due diligence allows for alternative avenues of compliance. For instance, Russia could have sought assistance from other States or international entities to address the situation, thereby avoiding a potential violation of its international obligations. This inaction raises concerns about the Federation's compliance with the principle itself, which obligates states to take reasonable steps to address harmful cyberattacks originating from their territory, regardless of the outcome. In conclusion, it is currently impossible to hold the Federation responsible for violating the obligation as outlined in Rule 13c of the GGE Report *on Responsible State Behaviour in Cyberspace* due to insufficient evidence and information.

Notwithstanding the fact that this specific case study is not a perfect example of the successful application of the due diligence principle in cyberspace, its primary relevance lies in highlighting cyberattacks that exploit the ground segment of a space system. This aspect is critical because it underscores the interconnected nature of space and cyberspace, which amplifies the vulnerabilities of space systems to cyber threats. As previously explained, this interconnection is significant from an international law perspective, as it allows for a focused application of the due diligence principle to a single domain—cyberspace—without necessitating an extensive evaluation of its application across both space and cyberspace. Moreover, what deserves more emphasis in the analysis is the practical application of the due diligence obligation to real-world events. Such exercises are invaluable for identifying the strengths and weaknesses associated with this obligation, thereby encouraging States to develop and promote consistent state practice in this area.

Conclusion

Given the increasing reliance of both civil society and the military sector on space services, it is imperative to mitigate, as much as possible, the vulnerabilities that could adversely affect these services. As demonstrated in this paper, the primary risks to these services currently stem from cyberattacks due to the growing interconnection between space and cyberspace. Moreover, technological advancements in both sectors render space assets simultaneously more vulnerable and resilient to cyberattacks, as technological development can be exploited for both peaceful and malicious purposes.

The due diligence obligation could play a crucial role in blocking and condemning cyberattacks that may partially or entirely, temporarily or permanently, compromise space systems, particularly their ground segments. As discussed throughout the sections of this paper, there are notable shortcomings in the current application of the due diligence obligation in cyberspace to effectively protect space systems. For instance, it may be necessary to further define the specific obligations arising from this principle, such as those outlined in Rule 13c. Adopting a broad and flexible approach to the measures that States can implement to avoid breaching this obligation could prove beneficial. Such an approach would clarify how to correctly apply and adhere to the obligation, thereby facilitating its implementation through national, regional, and international policies. Another issue that requires resolution is the attribution process. As previously emphasized, cyberspace is a domain where States and non-state actors can operate maliciously without being held accountable for their actions. To address this problem, it is essential to develop technical capabilities that facilitate the identification of the original source of an attack. In the invocation process of international responsibility for alleged violations of the due

diligence obligation, the technological process of attribution itself will play a pivotal role. Overcoming this limitation will significantly enhance the legal process of attribution. While in environmental law it is relatively easier to identify the State responsible for a wrongful act which violates due diligence, in cyberspace establishing this link between the conduct and the perpetrator is more challenging, due to the ease with which the source of an attack can be falsified. Once this problem is resolved, the application of the due diligence obligation will become more straightforward. Consequently, this will lead to a substantial reduction in the number of cyberattacks perpetrated by both State and non-state actors.
Finally, a clear process of interpretation and application of the provision is likely to result in an increase in state practice, ultimately leading to the recognition of the due diligence obligation in cyberspace as a customary norm.

Bibliography

BACE B. - YASIR G. - UNAL T., Law in Orbit: International Legal Perspectives on Cyberattacks Targeting Space Systems, in «Telecommunications Policy» 48 (2024).

BANNELIER-CHRISTAKIS K., Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations?, in «Baltic Yearbook of International Law»,14(2014), p. 5.

BIEIESEKER C., US and EU Officials Attribute Viasat Cyber Attack to Russia, Via Satellite, 2022. BOSCHETTI N., FALCON N., FALCON G., Space Security Lesson Learned from the ViaSat Cyberattack, in «ASCEND», (2022).

BRUMFIELD C., Incident response lessons learned from the Russian attack on Viasat, CSO, 2023,

CASARIL F. - GALLETTA L., Securing SATCOM user segment: A study on cybersecurity challenges in view of IRIS, in «Computers & Security», 140 (2024).

Charter Of The United Nations And Statute Of The International Court Of Justice, San Francisco 1945.

Council of Europe. Convention on Cybercrime (Budapest Convention), ETS No.185, adopted on 23 November 2001, entered into force on 1 July 2004.

Council of the EU. (May 10, 2022). Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union [Press release].

CZOSSECK C. - OTTIS R. - TALIHÄRM A.-M., Estonia after the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security, in «International Journal of Cyber Warfare and Terrorism (IJCWT)», 1(1), (2011).

Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC.

DoD Releases, DoD Commercial Space Integration Strategy, 2 April, 2024.

ERWIN S., Space Force to shore up cybersecurity as threats proliferate, Space News, 2022.

FLECK D., Searching for International Rules Applicable to Cyber Warfare—A Critical First Assessment of the New Tallinn Manual, in «Journal of Conflict and Security Law», (2013).

HEATHCOTE S., State Omissions and Due Diligence: Aspects of Fault, Damage and Contribution to Injury in the Law of State Responsibility, in Bannelier K. - Christakis T. - Heathcote S. (eds.), The ICJ and the Evolution of International Law: The Enduring Impact of the Corfu Channel Case, London-New York, Routledge, 2012, p. 308.

HITCHEN T., NATO plans first commercial space strategy to spur tech innovation, Breaking Defence, 2024.

Integrating Commercial Space for Military Applications in Europe: A Challenge and Opportunity, ESPI, 2024 (para. 5).

International Court of Justice, Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), February 26, 2007, ICJ Reports 2007.

International Court of Justice, Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. Albania), April 9, 1949, ICJ Reports 1949.

International Court of Justice, Pulp Mills on the River Uruguay (Argentina v. Uruguay), 20 April 2010,I.C.J. Reports 2010.

Italian Position Paper on International Law and Cyberspace, 2021.

KA-SAT Network cyber-attack overview, Via-Sat, 2022.

KAVALLIERATOS G. - KATSIKAS S., An exploratory analysis of the last frontier: A systematic literature review of cybersecurity in space, in «International Journal of Critical Infrastructure Protection», 43 (2023).

KENNY J., A general obligation of due diligence in international law?, European Journal of International Law, 2024.

KOIVUROVA T., Due Diligence, in R Wolfrum (ed), Max Planck Encyclopedia of Public International Law, 2010.

LIU Y.I., State Responsibility and Cyberattacks: Defining Due Diligence Obligations, in «The Indonesian Journal of International and Comparative Law», (2017).

LOMBARDO S., VPN: cos"è, come funziona e per cosa viene utilizzata una rete privata virtuale, Cybersecurity 360, 2022.

LYSÉN G., State Responsibility and International Liability of States for Lawful Acts: A Discussion of Principles, Coronet Books Inc., 1997.

MACHEN J., Zero trust" can secure satellite communications against cyberattack, Cybernet, 2019.

MARTINO L., Cyber e Spazio: nuovo fronte di difesa integrata, ISPI, 2022.

MCDONALD N., The Role of Due Diligence in International Law, in «Cambridge University Press» (2016).

MOSCATELLI L., Putin e putinismo in guerra, Salerno Editrice, 2022.

NAKASHIMA E., Russian military behind hack of satellite communication devices in Ukraine at war"s outset, say, The Washington Post, 2022.

NATO - Official text: Brussels Summit Communiqué issued by NATO Heads of State and Government (2021), 14-Jun.-2021.

NATO - Official text: London Declaration issued by NATO Heads of State and Government (2019), 04-Dec.-2019.

NATO - Official text: Madrid Summit Declaration issued by NATO Heads of State and Government (2022), 29-Jun.-2022.

NATO - Official text: Vilnius Summit Communiqué issued by NATO Heads of State and Government (2023), 11-Jul.-2023.

NATO - Official text: Warsaw Summit Communiqué issued by NATO Heads of State and Government (2016), 09-Jul.-2016.

NATO Science & Technology Organization. Science & Technology Trends 2023-2043: Across the Physical, Biological, and Information Domains. Volume 2: Analysis, 2023.

OLLINO A., Due Diligence Obligations in International Law, Cambridge University Press: Cambridge, United Kingdom, 2022.

OTTIS R., Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective, NATO Cooperative Cyber Defence Centre of Excellence, 2008.

PAVUR J. - MARTINOVIC I., SOK: Building a Launchpad for Impactful Satellite Cyber-Security Research, Oxford University, 2020.

ROSCINI M., Cyber Operations and the Use of Force in International Law, Oxford: Oxford University Press, 2014, pp.52-58.

SCHMITT M., NATO Cooperative Cyber Defence Centre of Excellence, Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge: Cambridge UP, 2013.

SKINNER B., Military Uses of Outer Space, SSI ISSUE GUIDE: ACCESS TO AND USE OF SPACE BY GLOBAL ACTORS, 2020.

SUWIJAK C. - LI S., Global Internet Access from the Low Earth Orbit: Legal Issues regarding Cybersecurity in Outer Space, in « Journal of East Asia and International Law » 15, (2022).

TALBOT JENSEN E., The Tallinn Manual 2.0: Highlights and Insights, in « Georgetown Journal of International Law 735», 48(2017).

The North Atlantic Treaty, Washington DC, April 4, 1949, NATO.

Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, 10 ottobre 1967.

UN Doc A/76/135, July 14, 2021.

United States General Accounting Office (GAO) Report, CRITICAL INFRASTRUCTURE PROTECTION Commercial Satellite Security Should Be More Fully Addressed, 2002.

VÄLJATAGA A., Cyber vigilantism in support of Ukraine: a legal analysis, CCDCOE, 2022.

VARADHARAJAN V. - SURI N., Security challenges when space merges with cyberspace, in «Space Policy», 67 (2024).

VILLANCE C., UK blames Russia for satellite internet hack at start of war, BBC News, 2022.

WINGFIELD T., The Law of Information Conflict, U.S. Dep't. of Defense, Dictionary of Military and Associated Terms, 2000.