SHIFT IN SPACE INSURANCE REGULATIONS AMID DUAL-USE, COMMERCIAL AND POLYCENTRIC SPACE ACTIVITY

Olga Sashko[a], Anna Hurova[b]*

[a] *Department of Tourism and Hospitality, Australia,*
[b] *Space Chair ENS-PSL, France*

Abstract

This research raises complex questions about how commercial spacecraft engaged in dual-use operations are protected through insurance. Space insurance has traditionally been structured around physical-damage triggers, supplemented by safety standards, risk-management obligations and general loss-mitigation duties. However, non-kinetic interference may cause prolonged service outages, contractual failure and loss of revenue without producing clearly attributable or permanent physical damage. Such losses, therefore, sit at the margins of insurability under prevailing 'all risks of physical loss or damage' policies. In this context, the space insurance market has suffered significant losses in recent years, with some insurers reducing capacity or exiting the sector altogether. This heightens concern that State-linked, systemic interference with dual-use satellites may be regarded by private markets as effectively uninsurable. Yet the risks themselves, given the dependence of critical infrastructure, essential services and national security on space-based services, cannot realistically be left uninsured or absorbed solely by commercial operators. Drawing on maritime war-risk insurance and emerging treatment of cyber and war perils in insurance wording, it contends that the insurability of strategic, politically driven losses has historically depended on public-private arrangements in which states assume responsibility for the catastrophic tail of the risk distribution. Applied to space, this supports the development of dedicated space war-risk and cyber-risk regimes, clearer delineation between commercial and sovereign risk, and limited government participation as insurer or reinsurer of last resort. Framed in this way, space insurance can be analysed as a mechanism through which States acknowledge, structure and govern vulnerability in an increasingly contested space domain. This research focuses on the allocation of risk between public and private actors in the dual-use space domain, with particular attention to criteria for assessing non-kinetic risks. It examines financial guarantee mechanisms as alternatives or complements to traditional insurance schemes in cases of damage, including salvage-type arrangements. Drawing on comparative analysis, the study explores maritime law precedents and assesses their potential adaptability to space activities. It further analyses divergent national approaches to insurance and liability coverage, with the aim of identifying a regulatory mechanism capable of balancing State responsibility with the protection of private operators' interests in space activities.

Keywords: insurance, dual-use, cyberattack, maritime war risk.

I. Introduction

Contemporary space systems possess inherent dual-use capability, enabling them to support both civilian and military functions simultaneously. Commercial Earth observation satellites provide imagery for agriculture, environmental monitoring and resource management while also possessing intelligence, surveillance and reconnaissance capabilities. Similarly, global navigation satellite systems support civilian transportation networks while also providing military positioning and targeting capacity. Space activities are also becoming increasingly defence oriented as a result of global geopolitical shift. One prominent example is the full-scale invasion of Ukraine. The war in Ukraine illustrates the growing strategic significance of commercial space infrastructure [1] . Commercial satellite systems and Earth observation providers have played an important role in supporting Ukrainian communications, situational awareness and operational coordination.

The conflict demonstrates the extent to which private space infrastructure may rapidly acquire strategic significance during periods of geopolitical tension, despite remaining commercially owned and operated. As commercial systems become integrated into defence-support functions, they may also become exposed to hostile interference, cyber operations and other forms of strategic disruption. The European Space Agency ('ESA') Report on Space Economy 2026 States that the share of government space budgets allocated to defence continued to exceed civil space spending in 2025, accounting for 53 per cent, and anticipates that government space budgets

may increase by more than 20 per cent from 2026, driven almost entirely by defence programs. At the same time, private investments in space ventures worldwide reached an all-time high of €11.7 billion in 2025 [2]. This shift reflects the increasing prominence of military component within the civil-military dual-usage of space. In this context, RAND suggests that stakeholders should assume the dual-use nature of space systems and avoid attempts to distinguish dual-use systems from non-dual-use systems [3]. Any satellite may therefore be perceived as capable of supporting military activity, increasing uncertainty and reducing transparency, confidence and predictability of potential risks. The increased integration of commercial systems into governmental and defence-support functions has important implications for risk allocation and insurance. Commercial operators may become exposed to hostile interference not because of their ownership status, but because of the functions they perform. Consequently, commercial satellites may become targets of cyber operations, electronic warfare, jamming or spoofing despite remaining civilian assets under private ownership. This increasing unpredictability complicates risk assessment and insurance.

The space insurance market has suffered significant losses in recent years, with some insurers reducing capacity or exiting the sector altogether [4]. This heightens concern that State-linked, systemic interference with dual-use satellites may be regarded by private markets as effectively uninsurable. Yet the risks themselves, given the dependence of critical infrastructure, essential services and national security on space-based services, cannot realistically be left uninsured or absorbed solely by commercial operators. Drawing on maritime war-risk insurance and emerging treatment of cyber and war perils in insurance wording, this paper contends that the insurability of strategic, politically driven losses has historically depended on public-private arrangements in which States assume responsibility for the catastrophic tail of the risk distribution. Applied to space, this supports the development of dedicated space war-risk and cyber-risk regimes, clearer delineation between commercial and sovereign risk, and limited government participation as insurer or reinsurer of last resort. Framed in this way, space insurance can be analysed as a mechanism through which States acknowledge, structure and govern vulnerability in an increasingly contested space domain.

This research raises complex questions about how commercial spacecraft engaged in dual-use operations are protected through insurance. Dual-use space activity has no yet clear identification in the law and policy documents, raising questions about the allocation of risk between public and private funds. [3] Under Article VI of the Outer Space Treaty (‘OST’), States Party of the Treaty bear international responsibility for national activity in outer space, including activities conducted by non-government entities. Article VII provides that a launching State is internationally liable for damage caused by its space objects to another State Party [5]. Neither provision, however, determines how that risk should be allocated through national insurance mechanisms.

The main hypothesis of this paper is that the uncertainty arising from dual-use space activities increases insurance risk and challenges insurability. In this context, the paper seeks to address the following questions: (1) how to consider dual-use space activities according to their insurability; (2) how to assess risks and losses affecting a space object and quantify the resulting physical and non-physical losses, including losses caused by cyber incidents and business interruption, which are generally not covered by first-party property damage insurance; and (3) how dual-use space activities could be insured in light of the general restrictions commonly applied to military and war-related risks in other sectors, such as maritime insurance. Drawing on comparative analysis, the study explores maritime law precedents and assesses their potential adaptability to space activities.

Furthermore, this research focuses on the allocation of risk between public and private actors in the dual-use space domain, with particular attention to criteria for assessing non-kinetic risks. It examines financial guarantee mechanisms as alternatives or complements to traditional insurance schemes in cases of damage. It further considers selected national approaches to insurance and liability coverage, with the aim of identifying a regulatory mechanism capable of balancing State responsibility with the protection of private operators’ interests in space activities.

II.1 Commercialisation and the Changing Risk Environment: Commercialisation and Polycentric Space Activity

Outer space has become increasingly embedded within the functioning of contemporary society and the global economy. Satellite-enabled infrastructure now supports communications, financial transactions, logistics, weather forecasting, environmental monitoring, emergency management and navigation services. Positioning, navigation and timing (‘PNT’) services provided by satellite systems underpin critical infrastructure across multiple sectors, creating a growing degree of dependence upon space-based services. [6].

This dependence has coincided with rapid commercialisation of the space sector. Whereas space activities were historically dominated by States and government agencies, contemporary space operations increasingly involve private corporations, public-private partnerships and commercially operated constellations. This transformation has

contributed to the emergence of an increasingly polycentric space environment in which both States and private actors now play significant roles in operating, supporting and shaping space activities.

Polycentricity shapes the interaction between these actors and, consequently, the legal and financial mechanisms by which their activities are regulated, within which insurance plays a key role. Polycentric governance refers to a network of independent nodes that can make decisions autonomously and coordinate among themselves to produce a joint outcome [7]. This increasingly reflects space governance and may further develop by building trust among actors, clarifying rights and expectations, encouraging broad participation, and resolving unavoidable disputes [8].

From this perspective, insurers are well positioned to make a meaningful contribution to the governance of space activities. Indeed, they inherently contribute to such governance by deciding whom they will insure and under what terms and conditions coverage will be provided. Furthermore, insurance models for high-risk ventures, including extensive reinsurance and quota-sharing regimes, which enable risk-sharing among syndicates (and "names") and facilitate the underwriting of very large risks while reducing the exposure of individual underwriters, demonstrate the significant role of insurance within polycentric space governance. [9]

II.2 Commercialisation and the Changing Risk Environment: The Evolving Space Risk Environment and Insurance Market Capacity

The scale of transformation of the space risk environment is significant. The global space economy is projected to triple to approximately 1.8 trillion by 2035 [10] . As space technologies are becoming progressively integrated into industries far removed from the traditional space sector, including food and beverage and retail, the economic significance of space is increasingly moving well beyond entities directly engaged in space activities and now encompasses sectors whose operations depend upon space-enabled services and infrastructure.

Commercial expansion has been facilitated by several technological developments, including reduced launch costs, satellite miniaturisation and the proliferation of low Earth orbit ('LEO') mega-constellations. These developments have lowered barriers to entry and accelerated the number of actors capable of conducting space activities. While these developments have expanded access to space, they have also contributed to a more congested, competitive and strategically contested operating environment. At the same time, the high cost of insurance, coupled with the relatively limited capacity of the insurance market, constitutes a significant barrier to market entry for emerging space companies. Space insurance developed in response to a relatively small number of highly complex and technologically sophisticated risks. Consequently, the availability of sufficiently large and homogeneous datasets capable of supporting conventional actuarial analysis remains limited [11].

This difficulty is compounded by the unique challenges associated with space environment, including increasing orbital congestion and the difficulty of predicting collision risks with precision [12]. The development of mega-constellations has introduced additional complexity because large numbers of interconnected satellites may need to be assessed as part of a broader operational system rather than as entirely independent risks. This increases the potential for correlated and cascading losses. [13]. These complexities complicate the accurate assessment and pricing of risk.

Their effect was illustrated by the space insurance market's experience in 2023, when approximately USD 1.43 billion in claims substantially exceeded estimated premium income of approximately USD 550 million. In response, approximately USD 160 million in launch and in-orbit capacity was withdrawn during 2024. Although capacity began to recover in 2025 and 2026, premium rates remained elevated and insurers continue to adopt a highly selective underwriting approach. Moreover, theoretical market capacity substantially exceeded the working capacity likely to be deployed in practice, particularly for LEO missions and risks lacking heritage technology or demonstrated technical reliability [14].

At a time when the motivations, governance, and objectives of space activities are undergoing profound transformation, it is essential that the insurance industry be capable of providing adequate coverage to support the sustainable development of the space sector. Commercialisation of space activities has also transformed the nature of insurance exposure within the sector. The implications of limited market capacity cannot, however, be separated from the changing nature of the exposure itself. Commercialisation has transformed the nature of insurance exposure within the space sector. Contemporary satellite infrastructure supports various mission-critical services upon which both governmental and commercial actors increasingly depend.

As a consequence, insurers are no longer assessing risk solely by reference to the potential physical failure of an individual spacecraft but must also consider the broader operational and economic disruption capable of arising from interference with space-enabled services. The increasing integration of commercial spacecraft into critical infrastructure and governmental support functions complicates the distinction between commercial and

war risk. Commercial satellite systems may remain privately owned and operated while simultaneously supporting communications resilience, navigation capability, intelligence functions or other services of strategic significance.

Consequently, commercial operators may become exposed to hostile interference or cyber operations not because of their ownership status, but because of the functions performed by the underlying space infrastructure [9] These developments contribute to a more complex risk environment in which losses may arise not only through physical destruction of spacecraft, but also through interference with operational continuity, data transmission and service availability. In this respect, contemporary space risks increasingly challenge traditional insurance frameworks structured primarily around physical loss or damage to insured property.

III.1. Dual-Use Space Activities and the Limits of Insurability: Approaches to define duality and their impact on the insurance

The distinction between civil and military space activities was not a primary concern at the time when the concept of the peaceful use of outer space was established. During that period, States were the principal actors conducting space activities, and the primary legal framework governing their conduct was the United Nations Charter rather than a distinction between civilian and military uses of space. Consequently, the legality of space activities was assessed mainly through the lens of international peace and security rather than according to the intended purpose of particular space objects. This situation has changed significantly with the reconfiguration of space governance resulting from the emergence of private space actors. Although international political risks have not disappeared, they have gradually been overshadowed by financial risks and commercial profitability. As the commercialization of outer space accelerates, increasing attention has been devoted to the legal and insurance implications of duality in space activities. There is no universally accepted definition of duality in space [3], but there are two principal approaches to how duality is distinguished.

The first concerns dual-use systems, namely systems that simultaneously or alternatively perform civilian and military functions. Their defining characteristic is that they actively perform both functions, potentially increasing their exposure to hostile interference because of their defence applications.

The second approach concerns dual-purpose objects, namely space objects developed for legitimate civilian objectives, such as active debris removal or on-orbit servicing, but possessing technological characteristics that could potentially be diverted to hostile actions, including robotic arms, rendezvous and proximity operations, or high manoeuvrability. Although these capabilities are technologically neutral, uncertainty regarding the operator's intentions creates a perception of threat [15]. Thus, while dual use refers to systems whose design and operation explicitly support both civilian and military activities, dual purpose describes systems intended for non-military missions that nevertheless possess latent military capabilities. The regulatory approach ultimately adopted is of considerable importance for the insurance sector, as it determines how insurers assess operational risks associated with space systems. In the absence of a clear definition, a behaviour-and effect-based approach may provide a more practical basis for classifying space activities.

The RAND Report suggests that stakeholders should pursue a framework based on “concrete activities” and “use of space system-collected date’ to mitigate risks of escalation or conflict. Factors that are often difficult to discern, including intent, user identity, and technical design, may be incorporated where they can be definitively established. [3]. Ioana Bratu and Frans von der Dunk similarly observed that distinguishing between purely civilian and exclusively military space assets or data may be increasingly impractical because "what constitutes a space threat cannot be identified by observing space objects, technologies or space capabilities in isolation, but by taking into account behaviour" [16]. It is noteworthy that the European Union Space Strategy for Security and Defence adopts a similar approach, recognising that most space technologies are dual-use and that space threats must be assessed by reference to behaviour rather than space objects, technologies or capabilities in isolation [17]. In current insurance practice, companies frequently manufacture satellites and related equipment in-house and either operate these assets themselves or provide hosted payload services to customers.

Insurance coverage is generally provided during the manufacturing process and throughout the different phases preceding launch [18]. Consequently, satellites and their individual components are generally covered by pre-launch insurance policies regardless of whether their future use is civilian or military. The legal and insurance position becomes more complex once a satellite is intended to perform dual-use functions.

Unlike ordinary manufacturing risks, operational dual-use activities may trigger exclusions traditionally applied to military risks and war-related activities. As a result, determining whether a space activity should legally be classified as civilian, military, or dual-use directly affects the assessment of insurable risks, the applicability of insurance exclusions, and ultimately the availability of insurance coverage. The difficulties associated with assessing and quantifying risk become particularly significant in this context.

A commercial satellite supporting government, military or critical-infrastructure functions may be exposed not only to conventional launch and operational risks but also to politically motivated cyber operations, jamming, spoofing and other forms of non-kinetic interference. Such events are difficult to quantify because of the limited claims history, problems of attribution and the possibility that a single operation may affect more than one spacecraft or a shared component of the space system. Underwriters have also started using satellite telemetry data and predictive analytics to refine their pricing models.

However, an insurer may be unable to obtain information that cannot be disclosed because of the military purpose of the activity. This may create an information asymmetry because the insurer is asked to assume an increased exposure without access to information ordinarily material to underwriting. It may consequently be difficult for the insurer to determine whether the risk is insurable and to price it accurately, potentially resulting in higher premiums, narrower cover or a refusal to insure the exposure. [19]

III.2. Dual-Use Space Activities and the Limits of Insurability: Non-Kinetic Threats and the Physical Damage Limitation

Space insurance has traditionally been structured around physical-damage triggers, supplemented by safety standards, risk-management obligations and general loss-mitigation duties. At the same time, the proliferation of space debris, the increasing software-driven complexity of space systems, the rapid expansion of private satellite constellations, and the adoption of United Nations General Assembly Resolution 77/41, Destructive Direct-Ascent Anti-Satellite Missile Testing [20], have significantly altered the contemporary space security landscape.

As the likelihood of kinetic attacks declines, particularly considering international efforts to discourage destructive anti-satellite missile testing, the probability of non-kinetic threats, especially cyberattacks, continues to increase.

Consequently, the notion of the dual use of space objects is becoming progressively associated not only with their physical characteristics but, more importantly, with their software architecture and cyber capabilities. Non-kinetic interference may produce different financial consequences. Cyber operations, jamming or spoofing may cause prolonged service outages, contractual failure and loss of revenue without producing clearly attributable or permanent physical damage. Quantification may therefore require consideration of the duration of the interruption, loss of revenue, additional operating and recovery expenses, data restoration costs and contractual liability. The fact that these losses can be quantified does not necessarily mean that they fall within the scope of the policy.

Business-interruption cover under a traditional property policy commonly depends upon interruption resulting from physical loss or damage. Where non-kinetic interference leaves the spacecraft physically intact, the resulting loss may therefore fall outside ordinary ‘all risks of physical loss or damage’ policies unless the relevant cyber exposure is expressly insured. [21], [9]

IV. War-Risk Exclusions

The absence of physical damage is not the only reason that a loss arising from non-kinetic interference may fall outside insurance cover. Even where the loss otherwise falls within the scope of cover, it may be subject to an exclusion. In the dual-use context, a war-risk exclusion is particularly relevant. Traditional property insurance policies commonly contain war-risk exclusions that remove cover for losses caused by war or warlike actions attributable to a State. Whilst such wording was developed in the context of conventional warfare involving the use of physical force, the exclusion may also be engaged where a loss arises from a State-linked cyber operation or other form of non-kinetic interference. [22]

The NotPetya coverage disputes and the subsequent tightening of war and cyber exclusion wording highlight the risk that State-linked interference with a dual-use space system may fall outside standard commercial insurance cover. The NotPetya incident involved malware widely attributed to Russia that was initially directed at targets in Ukraine but spread beyond them, causing substantial losses to private businesses operating in multiple jurisdictions. [23]. Mondelez International experienced two introductions of malware into its servers, causing widespread disruption across it networks. It subsequently sought more than USD 100 million under an all-risks property policy that expressly covered damage to electronic data, programs and software caused by malicious code, together with associated business interruption losses. [24] Zurich American Insurance Company (Zurich) relied on the war-risk exclusion clause to deny coverage for the losses arising from the attack. The relevant wording excluded loss or damage directly or indirectly caused by “hostile or warlike action in time of peace or war”, including actions by a government or sovereign power, a military force or an agent or authority of such a

party. [24] The case settled without a judicial determination of whether a State-linked cyber operation, conducted outside conventional armed hostilities and producing widespread incidental loss, constituted hostile or warlike action for the purpose of the policy. [25]

The related litigation brought by Merck provides some guidance, although does not fully resolve the issue. The New Jersey appellate Division held that hostile or warlike action exclusions did not apply to NotPetya cyberattack, emphasis that "the exclusion of damages caused by hostile or warlike action by a government or sovereign power in times of war or peace requires the involvement of military action". [26] Whilst the Appellate Division decision demonstrates the difficulty of applying wording developed for conventional warfare to a State-linked cyber operation, the settlement left the issue without a final determination by the Supreme Court of New Jersey.[26] The more significant development following the NotPetya disputes has been the revision of policy wording. Insurers, particularly within the Lloyd's market, have increasingly moved away from reliance on traditional references to war and warlike action in war-risk exclusions and have instead introduced bespoke clauses addressing cyber operations, cyber war and State-backed cyberattacks. [27] , [28]. Under these revised wordings, the assessment is no longer confined to whether an operation can be characterised as war or warlike.

Instead, consideration may be given to whether the operation was conducted as part of, or in immediate preparation for, a war; whether it is attributable to a State; whether it caused a State to become an "impacted state" within the meaning of the policy; and whether its consequences significantly impair the functioning, security capabilities or essential services of a State. Attribution is determined by reference to the objectively reasonable evidence available to the parties, which may include formal or official attribution by a government. [27], [28]. Applied to dual-use space systems, these criteria would direct attention to the government or defence functions performed by the satellite and the strategic importance of the affected services.

Depending upon the wording adopted, a cyber or other non-kinetic operation attributed to a State may fall within the exclusion because of its effect on those functions, even where the available evidence does not establish whether the satellite was targeted because of its civilian or defence use. [3]. In those circumstances, the dual-use nature of the satellite may therefore affect the characterisation of the resulting losses. The commercial operator may consequently be left with significant uninsured losses where it is not possible to separate losses affecting its commercial services from the exposure arising from its government or defence function. The fact that ordinary space insurance may exclude losses arising from State-linked interference does not necessarily establish that those risks are inherently uninsurable. It instead raises whether the exposure can be transferred through separate specialist cover and how losses beyond the capacity of private insurance should be allocated. The marine insurance market provides a useful point of comparison because it has historically separated ordinary marine risks from war risks and developed distinct mechanisms for insuring and pricing the latter, including arrangements involving State participation.

V.1 The Maritime Insurance Analogy: Marine War-Risk and Strikes Cover

Historically, the Ship and Goods ('SG') policy insured war risks together with ordinary marine risks. However, technological developments, together with conflicts in the late nineteenth century, caused marine underwriters to reconsider whether those risks should continue to be insured together. Subsequently, ordinary marine and war risks were generally insured separately [29]. Contemporary hull and cargo policies ordinarily exclude war, hostile acts, terrorism, strikes and other politically motivated perils from ordinary cover. These risks may instead be insured through specialist war and strikes clauses incorporated into the primary policy or under a separate war-risk policy. [30] This separation enables war and politically motivated risks to be underwritten and priced separately, with the premium and policy conditions adjusted to reflect the proposed route, timing of the voyage and prevailing geopolitical conditions. [31], [30], [32] The separation may nevertheless produce coverage gaps because specialist cover does not necessarily reinstate every peril excluded from the ordinary policy. For example, capture, seizure, arrest, restraint or detainment may be covered only where it arises from a specified war-related peril, while losses resulting from delay or frustration of the voyage may remain excluded. Cargo war-risk cover also generally attaches only when the cargo is loaded onto an overseas vessel and terminates upon discharge or shortly after the vessel's arrival. War-related loss during an inland stage of the transit may therefore remain uninsured unless additional cover is obtained. [33] Marine cargo insurers also use policy mechanisms that permit the price and availability of war-risk cover to respond to changing exposure during the policy period.

Although the initial premium under an annual cargo policy may include a component for war and strikes risks, additional premiums may be imposed where a shipment enters an area of heightened tension. For example, QBE's 2025 Marine Cargo Policy permits the insurer to vary its war and strikes rate upon seven days' written notice and to cancel that cover on seven days' notice, while generally preserving cover for risks that attached before cancellation became effective [34]. Munich Re similarly applies surcharges to shipments involving elevated or high-risk locations

and determines the availability, conditions and premium at the time of shipment for more severe risks. [35] These mechanisms allow insurers to continue evaluating and pricing the exposure as geopolitical conditions change. They do not, however, ensure that cover will remain affordable or available. A substantial premium increase, the imposition of narrower conditions or cancellation on short notice may transfer the financial consequences of an escalating conflict back to the insured when insurance protection is most important. Whilst repricing may preserve the insurer's willingness to provide cover, it may also place that cover beyond the financial reach of insureds. Cover may also be cancelled or withdrawn altogether as the exposure increases. [36] A similar mechanism operates in the marine hull war market.

The Joint War Committee, comprising underwriting representatives from the Lloyd's and International Underwriting Association company markets engaged in marine hull war business, publishes a list of geographical areas considered to present an enhanced risk of hull war, piracy, terrorism and related perils. Inclusion of an area does not itself determine the availability, price or terms of cover. Its application to an individual policy, including any additional premium, remains a matter for negotiation between the underwriter and broker. The list therefore identifies changes in exposure without prescribing the underwriting response. [37], [38]

The maritime model demonstrates that ordinary insurance policy need not absorb every politically motivated peril and that specified risks may instead be allocated to separately defined and priced cover. It also shows, however, that such separation is effective only where the exclusion under the ordinary policy and the corresponding specialist cover are sufficiently aligned. Otherwise, a loss may fall between the policies because of differences in the definition of the insured peril, the required causal connection or the period during which the specialist cover applies. Applied to dual-use space infrastructure, a specialist war-risk layer could permit State-linked and politically motivated interference to be assessed and priced separately from conventional launch and in-orbit risks. The relevant wording would need to specify whether it extends to cyber operations, jamming, spoofing and other non-kinetic interference occurring outside conventional armed conflict, as well as whether physical damage is required. It would also need to align with any cyber or war exclusions contained in the operator's ordinary space policy. The geographical component of the marine model is less readily transferable.

Unlike a ship entering a listed area, a satellite's exposure may change because of the functions it performs, the users it serves or its integration into governmental or defence operations, without any change in its physical location. Any equivalent variation mechanism would therefore need to respond to changes in the spacecraft's use and strategic significance, together with broader geopolitical conditions and the potential accumulation of loss across a constellation or shared infrastructure. Although such a mechanism may enable insurers to adjust premiums and conditions rather than immediately withdraw cover, it would also permit the insurer to increase the premium or cancel cover as the exposure changes.

Accordingly, specialist war-risk insurance may consequently become commercially unviable for the operator or be withdrawn altogether as the spacecraft assumes greater governmental or strategic significance. As the continued operation of such infrastructure may also be important to the State, this concern may, however, be addressed through government participation that supplements private insurance capacity.

V.2 The Maritime Insurance Analogy: Government Sponsorship and Reinsurance

The maritime insurance market provides examples of such government participation where private war-risk insurance has been insufficient or unavailable for strategically important activities. In the United States, for example, Chapter 539 of Title 46 of the United States Code authorises federal war-risk insurance and reinsurance where adequate insurance for waterborne commerce cannot be obtained from authorised commercial insurers at reasonable rates or on reasonable terms (46 USC § 53903 (2018) [39].

The Maritime Administration has administered this authority through a standby emergency mechanism intended to support the continued flow of United States foreign commerce. During the 1990–1991 Gulf crisis, the President authorised the Maritime Administration to write war-risk cover for commercial vessels when commercial cover could not be obtained on reasonable terms [40].

The scheme therefore preserved private-market primacy while providing public capacity where the continuation of strategically significant transport would otherwise have been threatened. The United Kingdom provides a related example.

The *Marine and Aviation Insurance (War Risks) Act* 1952 established a statutory fund and empowered the responsible Minister to insure or reinsure ships, aircraft and cargo against war risks. Current agreements with UK shipowners' mutual insurance associations provide 95 per cent reinsurance for British-registered merchant ships and larger fishing vessels and 100 per cent reinsurance for small fishing vessels against specified war risks arising from hostilities involving the UK. Any deficiency in the fund may be met by Parliament [41]. These

arrangements are not examples of government assuming every loss connected with military activity. They are targeted public-private structures. Commercial insurers retain underwriting and administrative functions, while the State provides additional capacity for specified risks or periods of heightened exposure where this is necessary to support national security and the continued operation of essential services.

The main lesson for space insurance is that government participation may be justified where disruption to essential satellite-enabled services would have significant public or strategic consequences and adequate private insurance cannot be obtained on reasonable terms. Such insurer-of-last-resort arrangements illustrate a polycentric allocation of responsibility under which a specialist insurance committee identifies changes in risk exposure, private underwriters determine the terms and price of cover, and the State provides additional insurance capacity where the private cover is unavailable or cannot be obtained on reasonable terms.

VI. Conclusions

The analysis of the space and insurance markets as dynamic and interconnected systems that mutually influence one another leads to several conclusions. The increasing complexity of the space sector, driven by commercialisation, the proliferation of dual-use activities, and growing cyber-dependency, can be accommodated within existing insurance frameworks, provided that these frameworks evolve to reflect the changing nature of space-related risks.

First, given the prevailing case-by-case approach to assessing the dual-use character of space activities, risk assessment should increasingly focus on the broader operational and economic disruptions that may result from interference with space-enabled services, rather than being limited to direct physical damage to the space object itself. For increasingly interconnected space infrastructure, the consequences of an incident may extend well beyond the affected satellite to disrupt communications, navigation, data services, or other critical activities dependent upon space systems.

Second, the emergence of non-kinetic, particularly cyber, threats require greater precision in the formulation and application of war-risk exclusions. The NotPetya case illustrates the relevance of considering a range of contextual factors when determining whether an incident falls within a war-related exclusion. These may include whether the operation was conducted as part of, or in immediate preparation for, a war; whether it is attributable to a State; whether it caused a State to become an “impacted state” within the meaning of the policy; and whether its consequences significantly impaired the functioning, security capabilities, or essential services of a State. Applied to space activities, such criteria could provide a more nuanced basis for distinguishing conventional operational risks from politically motivated or State-linked interference.

Third, the maritime insurance model demonstrates that an ordinary insurance policy need not absorb every politically motivated peril. War and dual-use risks may instead be allocated to separately defined and priced specialist coverage. This model also demonstrates, however, that such a division is effective only where the exclusion under the ordinary policy and the corresponding specialist coverage are sufficiently aligned. Applied to dual-use space infrastructure, a dedicated space war-risk layer could allow State-linked and politically motivated interference to be assessed and priced separately from conventional launch and in-orbit risks. Unlike a vessel entering a designated high-risk area, however, a satellite's risk exposure may change as a result of the functions it performs, the users it serves, or its integration into governmental or defence operations.

Fourth, where the separation of war and civilian risks between different insurance schemes proves impracticable or creates significant imbalances in risk allocation, a State-backed war-risk mechanism may provide a more appropriate solution. At the same time, to avoid placing an excessive burden on public finances, such a mechanism could be organised according to a polycentric allocation of responsibilities. Under this model, a specialised insurance committee could monitor and identify changes in risk exposure; private insurers would retain underwriting and administrative functions; while the State would provide additional capacity for specifically defined risks or periods of heightened exposure where necessary to safeguard national security and ensure the continuity of essential services.

References:

1. T. Ogden, A. Knack, et M. Lebret, « The Role of the Space Domain in the Russia-Ukraine War », Consulté le: 7 août 2026. [En ligne]. Disponible sur: https://cetas.turing.ac.uk/publications/role-space-domain-russia-ukraine-war

2. « ESA Report on the Space Economy 2026 ». Consulté le: 7 août 2026. [En ligne]. Disponible sur: https://space-economy.esa.int/article/339/esa-report-on-the-space-economy-2026

3. B. McClintock, D. Glickstein, K. Langeland, A. Agachi, M. Lebret, et K. Schwindt, « Navigating Duality in Space: Establishing a Foundational Understanding of Dual-Use Space Activities », juin 2026. Consulté le: 7 août 2026. [En ligne]. Disponible sur: https://www.rand.org/pubs/research_reports/RRA4003-3.html

4. « The Orbital Insurance Market: How Underwriters Are Pricing Constellation-Scale Risk », New Space Economy. Consulté le: 9 août 2026. [En ligne]. Disponible sur: https://newspaceeconomy.ca/2026/03/29/the-orbital-insurance-market-how-underwriters-are-pricing-constellation-scale-risk/

5. « The Outer Space Treaty ». Consulté le: 7 août 2026. [En ligne]. Disponible sur: https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introouterspacetreaty.html

6. « Positioning, Navigation, and Timing | Cybersecurity and Infrastructure Security Agency CISA ». Consulté le: 7 août 2026. [En ligne]. Disponible sur: https://www.cisa.gov/topics/risk-management/positioning-navigation-and-timing

7. L. Wesel et D. Lambach, « Tackling the Space Debris Problem: A Global Commons Perspective », présenté à 8th European Conference on Space Debris, 2021. Consulté le: 9 août 2026. [En ligne]. Disponible sur: https://conference.sdo.esoc.esa.int/proceedings/sdc8/paper/230

8. J.-F. Morin et B. Richard, « Astro-Environmentalism: Towards a Polycentric Governance of Space Debris », *Glob. Policy*, vol. 12, nº 4, p. 568-573, 2021, doi: 10.1111/1758-5899.12950.

9. [9] « Space Insurance and the Law ». Consulté le: 7 août 2026. [En ligne]. Disponible sur: https://www.e-elgar.com/shop/gbp/space-insurance-and-the-law-9781839105852.html

10. « The space economy is projected to reach $1.8 trillion by 2035 | McKinsey & Company ». Consulté le: 7 août 2026. [En ligne]. Disponible sur: https://www.mckinsey.com/featured-insights/themes/the-space-economy-is-projected-to-reach-1-8-trillion-by-2035

11. K. Malinowska, « Risk Assessment in Insuring Space Endeavours: A Legal Approach », *Air Space Law*, vol. 42, p. 329-347, mai 2017, doi: 10.54648/AILA2017022.

12. C. R. O. Forum, « Understanding and mitigating the impacts of space-related risks », The CRO Forum. Consulté le: 7 août 2026. [En ligne]. Disponible sur: https://thecroforum.org/understanding-and-mitigating-the-impacts-of-space-related-risks/

13. « Space insurance is moving beyond the single satellite model », Insurance Business. Consulté le: 7 août 2026. [En ligne]. Disponible sur: https://www.insurancebusinessmag.com/uk/news/breaking-news/space-insurance-is-moving-beyond-the-single-satellite-model-576741.aspx

14. « Q1 2026: Global Insurance Market Overview », Aon. Consulté le: 7 août 2026. [En ligne]. Disponible sur: https://www.aon.com/en/insights/reports/global-insurance-market-insights/q1-2026-overview

15. A. A. Ortega, « Not a Rose by Any Other Name: Dual-Use and Dual-Purpose Space Systems », *Lawfare*, mai 2023, Consulté le: 7 août 2026. [En ligne]. Disponible sur: https://www.lawfaremedia.org/article/not-a-rose-by-any-other-name-dual-use-and-dual-purpose-space-systems

16. I. Bratu et F. G. von der Dunk, « The EU Space Act Proposal and its Impact on the Dutch Space Ecosystem », 11 août 2025, *Social Science Research Network, Rochester, NY*: 5389410. doi: 10.2139/ssrn.5389410.

17. « A EU Space Strategy for Security and Defence for a stronger and more resilient EU - Defence Industry and Space ». Consulté le: 7 août 2026. [En ligne]. Disponible sur: https://defence-industry-space.ec.europa.eu/eu-space-strategy-security-and-defence-stronger-and-more-resilient-eu-2023-03-10_en

18. « Space Law: Europe », Lexology. Consulté le: 7 août 2026. [En ligne]. Disponible sur: https://www.lexology.com/indepth/space-law/europe

19. M. Swayne, « A Guide to Space Insurance: How Insurers Master The Risky Stuff For The Space Industry », Space Insider. Consulté le: 7 août 2026. [En ligne]. Disponible sur: https://spaceinsider.tech/2025/03/06/a-guide-to-space-insurance-how-insurers-master-the-risky-stuff-for-the-space-industry/

20. UN. General Assembly (77th sess. : 2022-2023), Éd., *Destructive direct-ascent anti-satellite missile testing: resolution*. New York: UN, 12. Consulté le: 7 août 2026. [En ligne]. Disponible sur: https://digitallibrary.un.org/record/3997622

21. « Methodological principles of insurance stress testing - cyber component - European Insurance and Occupational Pensions Authority ». Consulté le: 7 août 2026. [En ligne]. Disponible sur: https://www.eiopa.europa.eu/publications/methodological-principles-insurance-stress-testing-cyber-component_en

22. « Asking the Right Questions about War Exclusions in the Context of Cyber Operations ». Consulté le: 7 août 2026. [En ligne]. Disponible sur: https://www.guycarp.com/insights/2022/11/war-exclusions-in-the-context-of-cyber-operations.html?utm_source=chatgpt.com

23. « Summons to Appear: NotPetya and the War Exclusion Clause - The SAIS Review of International Affairs ». Consulté le: 9 août 2026. [En ligne]. Disponible sur: https://saisreview.sais.jhu.edu/notpetya-and-the-war-exclusion-clause/

24. Circuit Court of Cook County, Illinois, Law Division, *Mondelez International, Inc. v. Zurich American Insurance Company*, vol. 2018L011008. 2018. Consulté le: 9 août 2026. [En ligne]. Disponible sur: https://regmedia.co.uk/2022/11/02/pacer_mondelez_zurich_complaint.pdf?utm_source=chatgpt.com

25. « Mondelēz settlement in NotPetya case renews concerns about cyber insurance coverage | Cybersecurity Dive ». Consulté le: 7 août 2026. [En ligne]. Disponible sur: https://www.cybersecuritydive.com/news/mondelez-zurich-notpetya-cyber-insurance-settlement/636029/

26. « MERCK & CO., INC. v. ACE | 307 A.3d... | 261a3d53350 | Leagle.com », Leagle. Consulté le: 7 août 2026. [En ligne]. Disponible sur: https://www.leagle.com/decision/307240261a3d53350

27. Tony Chaudhry Underwriting Director, « State backed cyber-attack exclusions ». Consulté le: 9 août 2026. [En ligne]. Disponible sur: https://assets.lloyds.com/media/35926dc8-c885-497b-aed8-6d2f87c1415d/Y5381%20Market%20Bulletin%20-%20Cyber-attack%20exclusions.pdf

28. « Cyber War and Cyber Operation Exclusion Clauses », Lloyd's Market Association Bulletin. Consulté le: 9 août 2026. [En ligne]. Disponible sur: https://my.lmalloyds.com/WP/LMA_Bulletins/LMA21-042-PD.aspx

29. R. Aikens, « Wars and Laws: how war has influenced the development of the law of marine insurance », nº No. 583, MarIus, p. 51-62., 2024.

30. « Insurability as Power: Reframing Control in the Strait of Hormuz ». Consulté le: 7 août 2026. [En ligne]. Disponible sur: https://rsdi.ae/en/publications/insurability-as-power-reframing-control-in-the-strait-of-hormuz

31. L. Lesuis, « What is war risk insurance for cargo? - Charterama ». Consulté le: 7 août 2026. [En ligne]. Disponible sur: https://charterama.com/blogs/what-is-war-risk-insurance-for-cargo/

32. « Marine cargo insurance: War and strikes risks | Marsh ». Consulté le: 7 août 2026. [En ligne]. Disponible sur: https://www.marsh.com/content/marsh2/en_us/industries/cargo/expertise/cargo-war-strikes-risk.html

33. « Understanding Cargo War Risks », NTI Limited. Consulté le: 7 août 2026. [En ligne]. Disponible sur: https://www.nti.com.au/news-and-resources/news/2026/understanding-cargo-war-risks-2026

34. « Marine Cargo Policy ». Consulté le: 9 août 2026. [En ligne]. Disponible sur: https://www.qbe.com/media/qbe/apac/new-zealand/document-listing/2025/06/19/06/32/marine-cargo-policy-mca0425.pdf

35. « War & Strikes Updates ». Consulté le: 7 août 2026. [En ligne]. Disponible sur: https://www.munichre.com/specialty/global-markets-uk/en/solutions/cargo-insurance/war-strikes-updates.html

36. « Understanding Cargo War Risks », NTI Limited. Consulté le: 7 août 2026. [En ligne]. Disponible sur: https://www.nti.com.au/news-and-resources/news/2026/understanding-cargo-war-risks-2026

37. Joint Committee Circular, « JWC Listed Areas Hull War, Piracy, Terrorism and Related Perils ». Consulté le: 9 août 2026. [En ligne]. Disponible sur: https://lmalloyds.com/wp-content/uploads/2025/06/JWLA-034-Saudi-Arabia.pdf

38. « LMA - Joint War Committee ». Consulté le: 7 août 2026. [En ligne]. Disponible sur: https://lmalloyds.com/committee/joint-war-committee/

39. « 46 U.S. Code § 53903 - Insurable interests », LII / Legal Information Institute. Consulté le: 7 août 2026. [En ligne]. Disponible sur: https://www.law.cornell.edu/uscode/text/46/53903

40. « Annual Report of the Maritime Administration for Fiscal Year 1991 [MARAD 1991] ». Consulté le: 7 août 2026. [En ligne]. Disponible sur: https://rosap.ntl.bts.gov

41. « Marine and Aviation Insurance War Risks Fund account: annual report 2024 to 2025 », GOV.UK. Consulté le: 7 août 2026. [En ligne]. Disponible sur: https://www.gov.uk/government/publications/marine-and-aviation-insurance-war-risks-fund-account-annual-report-2024-to-2025