71st International Astronautical Congress (IAC) – The CyberSpace Edition, 12-14 October 2020.

IAC-20-E9,2.D5.4,6,x58403

How to Estimate Insurance Coverage for Cybersecurity Protection for Satellites: A Case Study

McLee Kerolle[a], Andrea Capurso[b]

a) Space Law & Policy Analyst, Space Generation Advisory Council, Caribbean Space Society, mclee.kerolle@spacegeneration.org

b) Junior Lawyer, Studio Legale Guarino, Via G. Caccini 1, Rome, Italy, capurso.andre@gmail.com

Abstract

Cybersecurity is critical to maintain the global economic and military infrastructure. The common denominator here is that the world's infrastructure rests on the use and capabilities of satellite technology. As a result, this paper proposes the creation of a detailed risk analysis standard to be applied among the global space insurance market with an emphasis on cybersecurity. The first section of the paper serves to establish background information in regard to current trends in the space insurance market with regards to satellite costs, as well as common cybersecurity threats. The emphasis on cybersecurity threats of satellites cannot be underestimated. As cyberattacks by hackers are becoming more prevalent, there needs to be a proactive rather than reactive approach addressing cyberattacks to satellite systems because of how integral satellite use is to everyday life. The next section continues with a comparative analysis between space insurance and the general cyber security insurance regimes. While there is overlap between space insurance and cybersecurity insurance it is imperative to present the distinction in regard to cybersecurity protection for satellites in orbit. This section finds that cybersecurity insurance generally offers a range of tools for organizations such as prevention advice and mitigation support to build resilience in cyber related incidents. However, the novel nature of constantly evolving cybersecurity risks remains challenging for insurers to quantify and cover. Conversely, the space insurance market is roughly divided into three types of coverage: prelaunch, launch, and in-orbit insurance. In addition, the inherently risky nature of the space industry means that no one insurer is willing to cover a satellite. Despite this unique industry, this section finds that the space insurance market appears to follow the 'hard' and 'soft' cyclicality of conventional markets. The third and final section takes a proactive approach and offers a case study on how to estimate cybersecurity insurance coverage in the case of satellites. As the launch of satellites are expected to increase in frequency and size, the purpose of this case study is to create a uniform risk assessment stand to be applied among the satellite industry. Due to the sensitivity of information that is associated with space insurance, this section takes liberties with what may be included in the typical space risk portfolio such as: the possibility of total losses accumulating when several satellites are launched together; and wide range of insured values coupled with high exposure to total losses.

1. Introduction

The availability of satellite imagery and increased communication channels through the satellite has motivated and enabled several non-state, as well as certain state agencies to gain access to data that was previously unavailable. The increased use of satellite technology is essential to the global infrastructure. A 2020 report in *business insurance* stated that as governments attempted to deal with covid-19 ransom-ware attacks jumped 148% from February to March[1].A 148% increase is no small feat; it is not surprising considering the level of difficulty for corporate security teams to protect data on home computers.

While it is still too early to determine the effects of cyberattacks in 2020, one thing is for certain, because satellites possess unique cybersecurity challenges that make them high profile targets, the satellite industry needs to take proactive steps to protect itself from hackers. It is not hard to imagine a future where defending against cyberattacks will be the basic ingredient for modern conflict. Rightfully so, because cybersecurity is critical to maintain the global economic

and military infrastructure. The common denominator here is that the world's infrastructure rests on the use and capabilities of satellite technology. If there is interference or a cyberattack on this architecture, it can easily lead to catastrophic consequences. As a result, this paper proposes the creation of a detailed risk analysis standard to be applied among the global space insurance market with an emphasis on cybersecurity.

The first section of the paper serves to establish background information on the current trends in the space insurance market with regards to satellite costs as well as common cybersecurity threats.

The emphasis on cybersecurity threats of satellites cannot be underestimated. There is no 'suit of armor' around the satellites. As cyberattacks by hackers are becoming more prevalent, there needs to be a proactive rather than reactive approach addressing cyberattacks to satellite systems. The failure to be proactive is going to lead to vulnerabilities that are not specific to a country or organization, but the entire satellite industry.

The next section continues with a comparative analysis between space insurance and the general cyber security insurance regimes. while there is overlap between space insurance and cybersecurity insurance it is imperative to present the distinction in regard to cybersecurity protection for satellites in orbit. This section finds that cybersecurity insurance generally offers a range of tools for organizations such as prevention advice and mitigation support to build resilience in cyber related incidents. However, the novel nature of constantly evolving cybersecurity risks still remain challenging for insurers to quantify and cover. Conversely, the space insurance market is roughly divided into three types of coverage: prelaunch, launch, and in-orbit insurance. Despite the inherently risky nature of the space industry this section finds that the space insurance market appears to follow the 'hard' and 'soft' cyclicality of conventional markets.

The third and final section takes a proactive approach and offers a case study on how to estimate cybersecurity insurance coverage in the case of constellations. As the launch of constellations are expected to increase in frequency and size, the purpose of this case study is to create a uniform risk assessment standard to be applied among constellations. Due to the sensitivity of information that is associated with space insurance, this section takes liberties with what may be included in the typical space risk portfolio such as: the possibility of total losses accumulating when several satellites are launched together; and wide range of insured values coupled with high exposure to total losses.

2. Cybersecurity in Space

According to allied market research, in 2018, the global cyber insurance market size was valued at an estimate of $4.8 billion and is projected to reach 28.6 billion by 2026 growing at a CAGR of 24.9% from 2019 to 2026[2]. To understand what this means in terms of risk and the satellite industry, we must first lay out the working definition of cybersecurity. As defined by the international telecommunication union cybersecurity is "the collection of tools, policies, security concepts… risk management approaches… and technologies that can be used to protect the cyber environment and organization"[3]. Here, the connection between cyber security and the space industry is worth explaining because it cannot be understated. at its very nature, satellite operations are dependent on technology that attract hackers and attackers from across the spectrum due to the various entry points in satellite systems. For instance, the use of long-range telemetry for communication with ground stations is a significant weakness common to most satellite systems[4]. The reason for this is because uplink and downlink systems are easy access for criminals because they're often transmitted through open telecom network security protocols[5]. Moreover, because space is such a critical asset towards the global infrastructure, the security of space-based infrastructure depends on the safety of earth-space interactions and the security of systems relying on data from space depends on the safety of space-earth interactions[6]. As a result, it follows that the increase of hackers also increases the risk of disruption to earth-space and space-earth.

2.1 Cybersecurity Threats

Generally, threats in the intersection of space and cybersecurity can be placed in five categories: kinetic physical, non-kinetic physical, electronic, cyber, and earth-based[7]. With electronic and cyberattacks being more readily used, these are the types of threats that the paper will address in terms of trends in the space insurance market. Dr. Patricia M. Lewis and David Livingstone of Chatham House provide a succinct

summary of what generally is encompassed in the type of cyberattacks on satellites including jamming, spoofing, hacking attacks on communication networks, targeting control systems, and attacks on the ground infrastructure such as satellite control centres. Possible cyberthreats against space-based systems include state-to-state and military actions; novice and expert hackers; well-resourced criminal organizations; terrorist groups; etc.

Over the years, we have seen cybersecurity incidents play out in several ways: in 2009, Iran was accused of jamming BBC's signal in its territory in order to disrupt broadcasting during popular movements; similarly, in 2010, North Korea was blamed for GPS signal jamming in South Korea; and Finland's civilian air navigation systems were interrupted by an electronic attack during a NATO exercise in 2018.

2.2 Cybersecurity Trends

In regard to current trends in the space industry, the reason why this paper focuses on the trends only in relation to satellite costs is due to the unique nature satelliteshave as a critical part of the space infrastructure. Depending on the purpose and function, many satellites are designed for long term use. As a result, the technology installed in satellites inevitably becomes obsolete and creates legacy problems. furthermore, in a classic example of having too many cooks in the kitchen, because several parties contribute to the development of the integrated systems for typical satellite operations it creates the unintended effect of increasing the systems' vulnerability. Consequently, the overall costs associated with cybersecurity are increasing.

While the space domain has always been militarized in some shape or form, it is worth noting that the trend is moving away from military and research towards the commoditization of space. The rapid rate of technology growth, results in cheaper, low-cost and reliable access to space. moreover, as what often happens in the space industry, this results in a culture where the cumbersome process of creating legislation/legal framework is not able to catch up to the rapid rate of technological growth. In fact, even cybersecurity measures are unable to update to meet the demands of cybersecurity. For this reason, this paper is continuing the line of many in the space industry. however, instead of calling for the implementation of a hybrid space and cybersecurity legal regime (although it is needed). This paper presents a uniform risk assessment standard that the industry can use to guide cybersecurity issues within the satellite sector.

3. Space Insurance & Cybersecurity Insurance: Issues and

3.1 The Space Insurance Market: Rules and Products

The insurance market related to space activities represents a crucial element in the exploration and utilization of outer space. It provides coverage of the risks to which a spacecraft is exposed during its lifecycle[8]. Without that, it would be hardly imaginable for the industry to withstand the enormous costs connected to space accidents.

The need for space insurance is also a corollary of the obligations set upon spacefaring Nations by the international space treaties. These obligations involve aspects of national liability for public and private activities beyond the atmosphere. The issue of liability is framed by the general framework developed at the international level by means, principally, of Article VII of the Outer Space Treaty (1967) and the Liability Convention (1972). In both treaties the matter revolves around who would be liable to pay damages caused by space objects and on what basis of fault. Nothing is said, however, on whether and to what extent insurance might (have to) cover a potential liability compensation. This aspect is left to national regulations: only under domestic implementation mechanisms usually appropriate insurance or financial guarantees are required from the private operator[9]. It can be said that the space insurance market developed as a response to the need of so-called "launching States" to get their money back if they would be held liable for damages caused by the activities of private actors. Thus, the business of insuring space activities expanded upon that need and nowadays represents a complex system offering a variety of products.

The three main insurance products related to the space market are: *pre-launch insurance*, which provides coverage for damages occurring at the manufacturer's premises, at the launch site until ignition and at all places in between; *launch insurance*, which covers damages to the satellite from when the rocket ignites for launch until it is safely in orbit, and *orbital insurance*, which covers

events affecting the satellite while it is providing its service from Space.

For the purpose of this paper, the focus will be on the latter. It is, in fact, during their operational phase that space assets are more vulnerable to cyber interference and, potentially, to an interruption of business caused by hackers. Therefore, this Section of the paper intends to take a look at the main aspects of *in-orbit insurance* and analyze those elements of *cyber insurance* that play a role in the insurance market related to outer space.

3.2 Orbital Insurance: the Issue of Cyber Attacks

It is necessary to begin by looking at the scope of application of insurance policies.

Nowadays, an average coverage takes into account damages caused during the pre-launch and launch phases, the ones that historically expose satellites to the highest amount of risks and, when orbital insurance is provided, damages caused by objects in the hostile space environment (e.g. collisions) or by other events related to space weather (e.g. radiations). A comprehensive orbital insurance however shall today include also the risks coming from the cyber domain. Cyber attacks are, in fact, hardly included in orbital insurance policies, but their exclusion can represent a growing concern for stakeholders.

From a purely statistical perspective, there are events that are much less frequent, but always insured: collisions. They fall under the so-called "liability insurance", a form of third-party insurance applicable also during the orbital phase.

While satellites are in the hazardous extra-atmospheric domain, they can be involved in many events damaging other subjects, in Space or on Earth (e.g. hits by space debris, uncontrolled deorbiting, wrongly conducted maneuvers in proximity of other satellites, etc.). In these cases, the injured parties pressing for compensation under the international regime of space liability may cause significant financial losses to the satellite operator[10], unless the latter has liability insurance.

However, collisions between space objects are rare[11]. Of the 290 in-orbit fragmentation events that have been recorded since 1961, only a few were collisions (fewer than 10 accidental and intentional events); the majority of the events were explosions of spacecraft and upper stages[12].

Compared to actual collisions, cyber threats have in recent times worryingly increased. The history of hacks and interferences affecting space objects is long and dates back to the '90s.

One of the first scenarios played out in 1998 when hackers took control of the U.S.-German ROSAT X-Ray satellite. They did it by hacking into computers at the Goddard Space Flight Center in Maryland. The hackers then instructed the satellite to aim its solar panels directly at the sun. This effectively fried its batteries and rendered the satellite useless. The defunct satellite eventually crashed back to Earth in 2011. Hackers could also hold satellites for ransom, as happened in 1999 when hackers took control of the U.K.'s SkyNet satellites. Over the years, the threat of cyberattacks on satellites has gotten more dire. In 2008, hackers, possibly from China, reportedly took full control of two NASA satellites, one for about two minutes and the other for about nine minutes. In 2018, another group of Chinese state-backed hackers reportedly launched a sophisticated hacking campaign aimed at satellite operators and defense contractors. Iranian hacking groups have also attempted similar attacks[13].

Despite the ease for satellites to be targeted by a cyber-attack (as already explained in Section 1), the insurance market has been reluctant to include such threats into its policies.

In theory, they represent a typical event that would fall under *property insurance*. The latter usually takes into consideration physical loss, damage, or failure of the insured satellite while in orbit[14]. Indeed, cyberattacks can cause all three, severely affecting the worth of the targeted space asset[15]. Nonetheless, they are usually excluded from coverage thanks to the "war, terrorism and crime" clause.

It can be said that insurance is intended to cover only unforeseen and unforeseeable occurrences (e.g. random failures). Coverage is provided for just about anything that can go wrong with the satellite. "All perils" is the traditional expression. Mechanical or electrical failures, debris or meteoroid strikes, and the effects of space weather are all covered under a typical space insurance policy[16]. In other words, cyber attacks represent one of the very few events that are excluded from coverage.

The reasons behind this approach as well as the meaning of the "was, terrorism and crime" clause are not specific

of the space insurance business. They are rooted in the cyber world and the insurance products that have been developed as a response to the risks and threats of that domain. Therefore, they will be further explained below at Section 3.5, in the part of the paper dedicated to cybersecurity insurance.

3.3 Orbital Insurance: A "Structural" Problem

The exclusion of cyberattacks from the scope of applications of insurance policies is not the only troublesome factor for stakeholders. Insurers are facing a much more "structural" problem: the number of (un)insured satellites, which creates negative repercussions on activity and premiums.

In June 2019, a report[17] issued by the insurance company AXA XL stated that 43% of GEO satellites are insured on orbit and 25% of GEO operators buy little or no in-orbit insurance beyond 1st year in Space. As for LEO, only 6% of satellites have orbital insurance. Overall, the market is looking at 86% of the active satellites being uninsured while operating in outer space.

With these numbers, the premiums paid in the past years have been insufficient to cover the so-called "peak insured value", i.e. the maximum amount an insurance company has to pay if an insured asset is deemed a total loss. As a consequence, the business of insuring satellites has been regarded recently as unsustainable. This was the view of the insurer Swiss Re, which decided to exit the Space market in 2018[18].

Usually, an insurance business is built on high volume, low value, and predictability. Life insurance, for example, relies on large numbers of people paying small sums over time and dying within a fairly standard age range.

"Space is the exact opposite. You have twenty commercially-insured launches a year, that's it. Worldwide, it's basically a catastrophe business" – said Mark Quinn, now CEO of global insurance broker Willis' space division – "you're looking at one loss that can give you a hit of $400 million, and annual market premium is $750 million. One loss that burns more than 50% of the annual income for the entire market"[19].

In other words, the problem is that many stakeholders, from governments to private companies, do not underwrite insurance contracts. The result being that just one major accident in outer space could cripple the whole sector.

This deficiency of the orbital insurance market requires a change of direction.

Even more so, now that innovative space applications and technologies are carrying with them new risks and threats, stressing the satellite industry as a whole[20]. Thanks to the commercialization and democratization of the extra-atmospheric domain, more actors every year are able to take part in the exploration and utilization of outer space, benefitting from the new ways of conducting space activities (e.g. space constellations or cube-satellites[21]). At the same time, the insurance market is trying to adapt to these rapid changes. It has evolved from simple launch coverage to a complex discipline combining contract analysis and advice, risk evaluation, alternative risk transfer concepts, insurance program design and implementation, and claims negotiation[22]. Such evolution is a first step towards a more sustainable market. But the increased diffusion of underwriters will be key, because the ability of the whole satellite business to grow is inevitably linked to its ability to manage risk.

3.4 Conclusions on Orbital Insurance

The exclusion of cyberattacks from insurance policies and the limited diffusion of insurance products among space operators represent two critical gaps for the extra-atmospheric insurance market.

In order to increase the number of insured satellites in orbit, a crucial role may be played by national legislations which can impose insurance requirements on private operators in order to obtain and maintain the necessary license. Many space-faring Nations have put in place such mechanisms. However, the focus has been traditionally brought on third-party liability insurance, leaving product insurance often overlooked[23].

On the other hand, the problem of the exclusion of cyber-attacks from insurance policies is connected to the thorny issue of "attributability" in the cyber domain. Considering that this issue is a traditional aspect of cyber activities, its analysis together with its implications on the insurance business are carried on in the next part of the present Section.

3.5 Cybersecurity Insurance

"*Legal disputes regarding the validity of insurance claims will continue, and the combination of non-affirmative cyber coverage and the war exclusion leaves satellite operators with potentially inconsistent coverage in certain claims scenarios*". ~ Richard Parker, Assure Space [24]

Now that the previous sections have given an overview of space insurance, the type of cyberattacks that satellites are susceptible to, and a brief definition of cybersecurity, this section takes a more in-depth look at cybersecurity insurance. Similar to space insurance, there is no international regime or governing body that regulates cybersecurity insurance. While the International Telecommunication Union is a United Nations agency that serves to regulate frequencies of satellites as well as register the orbit of satellites, beyond that it has established very few standards.[25] Let alone standards that address cybersecurity.

While cybersecurity insurance has existed since the 1990s, as an industry it is still technically at its infancy. At its most basic form, cybersecurity insurance is offered to individuals and businesses in order to protect them from the effects and consequences of cyberattacks. While the cybersecurity insurance is nascent, according to the German reinsurance company Munich Re, worldwide spending on cyber-insurance is estimated to increase to US8−US9 billion by 2020[26] Moreover, in regards to cyberattacks, Cybersecurity Ventures estimated that the cost of cybercrimes to the world will increase to US$6 trillion annually by 2021.[27]

Despite the fact that the cybersecurity industry is still developing, the United States has the most advanced cybersecurity market in the world. For instance, in 2016 the U.S. and Europe accounted for $3 billion and $300 million, respectively, of $3.5 billion in global cyber-insurance premium. (see table 1)[28]

Table 1. Cyber-insurance markets in some key economies.

Economy	Cyber-insurance premiums	Total insurance premiums (US$, billion)	Cyber-insurance premiums as a proportion of total insurance premiums
Brazil	US$645,800 (2016) (https://tinyurl.com/yc6u4ap4)	58.9 (2016)[a]	0.001%
Germany	US$105-117 million (https://tinyurl.com/y8ypu8jw)	327.3 (2016)[a]	0.03%
India	US$ 27.9 million (2017) (https://tinyurl.com/y84jgxm2).	69.8 (2016)[a]	0.04%
Japan	Japan Network Security Association's estimate: US$134.2 million (2017) (https://tinyurl.com/y8l4jxlz)	407.4 (2016)[a]	0.03%
South Korea	US$26.4 million (2016) (https://tinyurl.com/yafs4p27).	185.6 (2016)[a]	0.01%
The U.S.	Verisk: commercial cyber-insurance market: US$ 6.2 billion by 2020 US$ 2.5 billion in 2016 (https://tinyurl.com/ydf7z28s).	2703.8 (2016)[a]	0.09%

a. *OECD. Gross insurance premiums, https://data.oecd.org/insurance/gross-insurance-premiums.htm.*

Similar to space insurance, cybersecurity insurance provides for first-party insurance and third-party insurance. First party cybersecurity insurance focuses on compensating or mitigating the costs of the policyholder. While third-party insurance covers the business and people that are found to be "responsible" for a breach.[29] In addition, insurers may encourage the policyholder to add "Errors and Omissions" coverage for added protection.

Unfortunately, unlike space insurance, cybersecurity insurance cannot be analyzed in a straightforward manner that couldn't be further from the truth. There are several challenges that keep the cybersecurity insurance market in this precarious position. The most pressing issues to cybersecurity to discuss in the section include the lack of standardization of the cybersecurity insurance market and the high uncertainty in pricing cybersecurity risks.

The lack of standardization of the cybersecurity insurance means that policyholders are required to have a clear understanding of their cyber risk exposures to determine the type of coverage required, as well as the amount of coverage based on the situation. In fact, according to a survey by Marsh &McLennan 49% of policyholders said that they had "insufficient knowledge" about their cyber risk exposures to assess the type and coverage of insurances they need[30].

In the case of the satellite industry, insufficient knowledge can amount to what Richard Parker of Assure Space describes as a "*lack of alignment in coverage intent across the [insurance] industry*"[31]. In 2017, the NotPetya cyber attack targeted dozens of companies in Ukraine, Europe and the United States. At the time, the

White House described this attack as the "most destructive and costly cyber-attack in history"[32]. Citing the 'war exclusion' that protects insurers from paying claims related to war damage, insurers declined to pay claims. What is concerning here is that the same war exclusion policy exists in all space insurance policies industry. Considering that there is no legal definition of cyber warfare, one space insurance expert expects most disputes to be resolved in court.

As stated in Section 1 access to the data and information on satellite coverages and losses are scarce to the general public. However, it is not only scarce to the public, but to the insurers as well. The lack of data makes it difficult to estimate the costs of cyberattacks. Moreover, it also becomes difficult for companies to measure the nature and extent of cyber-related exposure in order to make decisions as to what coverages for how much to purchase.[33]

Due to this uncertainty in pricing cyber risk coverage, insurers tend to be conservative and overcharge for cyber risk coverage. What this paper proposes in the case study is a way to remedy this uncertainty in pricing by proposing a standard that combines pricing models with legislative elements.

4. Case study

The nature of the true difficulty of creating a cybersecurity risk assessment standard for constellations (or individual satellites) lies in the fact that there are very few examples to use as a frame of reference. As a result, it becomes difficult to develop a complete framework for optimizing risk management and insurance for on-orbit servicing. Here, this section creates a relatively new framework for modeling and pricing cybersecurity risks and applies it to the case study as follows:

4.1 Threat Landscape

The number of space companies launching constellations are increasing while becoming prime targets for cyberattacks. As stated in the beginning of this paper, the development of the integrated systems for typical satellite operations creates the unintended effect of increasing the systems' vulnerability. It follows that the increase in numbers of constellations results in the increased vulnerability of these satellites. The potential damage from a cyberattack would be significant. As a result, these constellations are challenging the existing business paradigms for satellite insurance.

4.2 Challenge

The satellite industry provides essential services and any service disruptions could have a significant impact to a significantly large user base. Space123, an aerospace company, wants to launch its first set of 60 satellites for their satellite internet constellation MarsLink. SpaceXYZ is looking to achieve a better understanding of its cyber threats, balance sheet exposure and examine methods to mitigate and transfer their cyber risks[34].

4.3 Solution

While the information regarding satellite underwriters and premium are limited, there is solace in the fact that the satellite insurance has been around for 50 years. Conversely, while cybersecurity risks have been increasing in the last decades, the modeling of cybersecurity risks is still limited in its infancy. Global firm Aon presents a detailed step of the space insurance procurement process. After presentation of the risks, where all material facts for the parties are disclosed, the underwriter then conducts an in-depth study of the risk considering such factors as:

- The satellites model contracted
- The formula used to calculate when a loss has occurred
- The intended mission, the type of coverage requested, the value to be insured
- The value to be insured
- The risk portfolio currently underwritten by any given insurer
- The year's claims-to-premium ratio[35]

For instance, in the case of a satellite launch, a space insurance broker will take the combination of a satellite model with a low historical fail rate and match it with a launch vehicle with a high number of consecutive launches.[36] Here, the reason for this is because it allows the insurance broker to attract a more competitive rate as opposed to a rate with a new spacecraft model which launches on a launch vehicle with an inferior success rate.

As stated earlier, the most common type of space insurance deals with the actual launch covering risks that typically occur during the launch phase.

In a remarkable paper titled *Cybersecurity Insurance: Modeling and Pricing*[37], authors Maochao Xu and Lei Hua propose the use of a simulation approach, specifically the Monte Carlo simulation, to evaluate the 'security level' of a network and calculate the insurance premium for cybersecurity risk[38]. The benefit of their framework is that it not only models general infection (i.e. cyberattacks) and recovery processes but also related losses. As a result, the security of a network is evaluated based on estimates of the number of incidents, infection probabilities of nodes, and total loss.

When applying this approach to modeling and pricing cybersecurity risk for insurance purposes, practical issues are likely to arise regarding the size of the network and statistical inference. Addressing the size of the network first, the issue stems from the fact that the use of simulations to evaluate the 'security level' of a network is a time-consuming process. For companies that have a large-scale network, extensive simulations might prove too time-consuming to be practical. Yet, Xu and Hua found that infection probability is *heavily dependent* on the node degree and the recovery rate has a *significant effect* on the premium. As a result, in situations where a simulation is not feasible, such as when a company has a large-scale network, stationary probabilities can be used for approximation[39].

Regarding statistical inference, large-scale networks tend to have a high number of dimensions (i.e. attributes) which poses a challenge to statistical inference[40]. Fortunately, Xu and Hua provide several strategies for conducting a statistical inference. One strategy focuses on recovery and infection distribution. The proposed framework requires relevant data on the recovery time and infection type to be implemented because they are used to estimate the time-to-infection distribution[41]. Here, recovery time is directly related to the company's recovery capacity, which means it is relatively easy to collect the necessary data. This data can be then used to fit the *recovery distribution* using the *maximum likelihood estimation.*

Another strategy for conducting a statistical inference focuses on high-dimensional dependence. The dependence among cybersecurity risks is challenging because the dimension is massive. The common approach used to manage 'high-dimensional dependence' is to use a vine copula (multivariate cumulative distribution function), which is a graphical tool[42]. Still, the lack of cybersecurity risk data could make it difficult to estimate correlations. As a result, Xu and Hua conclude that there needs to be more research into the dependence modeling of an epidemic spread and hope that more attention is paid to the *dependence effect*.

When a space insurance company wants to offer cybersecurity insurance for a small satellite or constellation, a crucial step is to understand the evolution and spread of an epidemic over the network as the infection will cause losses in practice. It is also important for the insurance company to know the total loss during a specific period because premiums are determined based on the loss. While cybersecurity insurance alone may not be able to rectify this, when you analogize to the space insurance industry there may be an avenue to combine both regimes and apply that to create a cybersecurity risk standard for satellites.

As stated in Section 3.5 there is no international uniform space insurance regime. However, national policy does exist that may be able to address how insurance providers can cover satellites for cybersecurity risks. In 2015, the Netherlands' Innovative Solutions in Space B.V. (ISIS) and Innovative Space Logistics B.V. developed the world's first declaration based third-party legal liability (TPLL) policy for small satellites[43]. According to Dr. Neta Palkovitz this means that the number of satellites are insured under the same policy terms with the ability to add or omit satellites in a future date. It is undeniable, as Dr. Palkovitz has stated that this type of policy is perfect for constellations and swarms of satellites[44].

The advantage of this type of policy/model is two-fold because: 1) this model makes insurance coverage affordable to operators (which of itself is a key advantage in the small satellite market) and 2) the flexibility of adding new satellites and removing older satellites due to the fact that the operator will negotiate the policy once. Moreover, in her book *Regulating a Revolution: Small Satellites and the Law of Outer Space,* Dr. Palkovitz sheds light on the fact that advancements similar to TPLL have been made regarding property damage. This is important because as the complexity of satellite technology increases, the risks and the demand to insure these satellites increases. As Dr. Palkovit stated:

"*The combination of third-party liability insurance*

and property insurance allow private entities to gain some control over the legal and financial proceedings in case they cause or suffer damage"[45].

Applying this standard to create a uniform risk standard is game changing because it will indirectly cover the evolving nature of cybersecurity threats. Specifically the emergence of cyber-physical attacks; a unique cyberthreat that poses the risk of bodily injury to third parties[46].

5. Conclusion

Lloyd's Market Association (LMA), which represents the interests of the Lloyd's insurance community, recognizes the need to address the potential of a cyber-attack on satellites. As a result, they recently proposed model policy clauses to use as guidelines for insurers, brokers and satellite operators. According to Richard Parker of Assure Space, the purpose of the clauses in the new model is to clarify cyber coverage for satellite operators and address the issue of "silent" or non-affirmative coverage for cyber-caused risks[47].

The theme here is that it is imperative that the industry come with some type of standard, or guidelines such as LMA, to protect satellite operators from inconsistency of the insurance industry and uncertainty in pricing models. What this paper ultimately concludes is a type of hybridization where cybersecurity insurance elements are combined with space insurance elements. Specifically, while combining the Monte Carlo simulation to evaluate the 'security level' of a network and calculate the insurance premium for cybersecurity risk with third-party legal liability as codified in the Dutch Space Act. Suggestions, proposals, and papers such as this calling for a type of standardization for cybersecurity insurance will only increase as the space industry continues to grow. Hopefully some standard will be created before inaction hinders the industry.

[1] Thomson Reuters, *Hacking against firms surges as workers take computers home*, 17 April 2020, on BusinessInsurance.com, available online at: https://www.businessinsurance.com/article/20200417/NEWS06/912334100/Hacking-against-firms-surges-as-workers-take-computers-home-COVID-19-coronavirus# (this and all other websites cited herein have been last accessed in September 2020).

[2] A. Goswami and others, *Cyber Insurance Market by Company Size (Large Companies and Small & Medium-sized Companies) and Industry Vertical (BFSI, IT & Telecom, Retail & E-commerce, Healthcare, Manufacturing, Government & Public Sector, and Others): Global Opportunity Analysis and Industry Forecast, 2019–2026*; March 2020, available online at: https://www.alliedmarketresearch.com/cyber-insurance-market.

[3] N. Al-Rodhan, *Cyber security and Space Security*,May 26, 2020, available online at: https://www.thespacereview.com/article/3950/1?fbclid=IwAR2kZ3zZwWTvC0K2hXZQbkiH0mC48buTLOl1ciaOwRI4JH2Kf7j_LPsQTR8.

[4] F. Knott; *Cyber Concerns for the Satellite Sector*, 13 July 2020, available online at: https://www.attilasec.com/blog/satellite-cybersecurity#:~:text=Satellites%20and%20cyber%20risk,of%20potential%20inroads%20for%20hacking.

[5] See F.Knott, above at 4.

[6] See N. Al-Rodhan, above at 3.

[7] Ibid.

[8] M. Zajac, *Overview of Space Insurance*, published in the French review "Risques" vol. III, 1 Dec. 2017, pp. 42-46.

[9] A. Kerrest and others, *Liability and Insurance in the Context of National Authorisation*, published as chapter 4 of National Space Legislation in Europe: Issues of Authorisation of Private Space Activities in the Light of Developments in European Space Cooperation, Studies in Space Law, volume 6 (Frans G. von der Dunk, editor), Leiden, The Netherlands: MartinusNijhoff Publishers, 2011, pp. 125–161.

[10] That is due to the fact that such liability claims are connected to the cost of space activities and can therefore amount to hundreds of millions of dollars. In addition, when the damaged party has been injured on Earth, the satellite operator is liable regardless of fault. In fact, the liability regime for space activities – as provided by the Liability Convention of 1972 – revolves around a double standard of liability: absolute liability for damages caused by space objects on the surface of the Earth or to aircrafts in flight (Art. II); fault-based liability in the event of damage being caused elsewhere than on the surface of the Earth to third-party's space object or to persons or property on board (Art. III).
For more on this see A. Kerrest above at 9.

[11] At the same time, it cannot be denied that in the future the risk of collisions will increase. This is due to two main factors: 1) Space has become a crowded and congested domain, where many actors – public and private – carry on their activities in an intricate nest of orbits and frequencies; 2) the long presence of humans in outer space has created a dangerous amount of debris orbiting next to active satellites with an ever-increasing risk of collisions. As a consequence, an increased need for liability insurance will follow.

[12] The first recognized collision dates back to 1991 It involved a Russian non-functional navigation satellite, Cosmos 1934 and a piece of debris from a sister spacecraft, Cosmos 926. It was followed in 1996 by a collision involving a French CERISE spacecraft and a fragment from the third stage of an Ariane 1 launch vehicle, which had exploded ten years earlier. Most recently, in 2009 the world witnessed an accidental in-orbit collision between two satellites at 776 km altitude above Siberia. A privately owned American communication satellite, Iridium-33, and a Russian military satellite, Kosmos2251, collided at 11.7 km/s. Both were destroyed, and more than 2300 trackable fragments were generated, some of which have since reentered (that is, decayed and reentered the atmosphere, where they have burnt up).
See ESA, *About Space Debris*, available online at:
https://www.esa.int/Safety_Security/Space_Debris/About_space_debris#:~:text=More%20than%20290%20in%2Dorbit,of%20spacecraft%20and%20upper%20stages.
For more info on the history of collisions see:
https://www.orbitaldebris.jsc.nasa.gov/.

[13] W. Akoto, *Hackers could shut down satellites -- or turn them into weapons*, 12 February 2020, available online at:
https://gcn.com/articles/2020/02/12/hackers-satellites.aspx.

[14] Property insurance is basically granted as a product guarantee whose final aim is to refund the satellite's value. In other words, when the satellite ceases to function as it was designed to, property insurance can represent a safety net for the operator who doesn't have to directly bear the costs of its loss. As described by Victoria Samson of the Secure World Foundation in 2018, "the vast majority of all satellite ventures carry property insurance, which is typically the third-largest expenditure behind launch and manufacture". See V. Samson and others, *Can the Space Insurance Industry Help Incentivize the Responsible Use of Space?*, presented at the 69th International Astronautical Congress (IAC), Bremen, Germany, 1-5 October 2018, p. 3.

[15] For a simple communications relay satellite, the lost value will be in terms of transponder-years. For an imaging satellite, the process of establishing the loss quantum will involve the evaluation of performance parameters relating to image quality and/or quantity. See R. Gubby and others, *Preparing for the Worst: The Space Insurance Market's Realistic Disaster Scenarios*, in New Space, Vol. 4, No. 2, 2016, p. 99.

[16] Ibid.

[17] AXA XL, *2019 Space Insurance Update*, 2019, available online at:
https://iuai.org/IUAI/Study_Groups/Space_Risks/Public/Study_Groups/Space_Risk.aspx.

[18] C. Henry, *Big claims, record-low rates: Reshaping the space insurance game*, on SpaceNews.com, 6 September 2019.

[19] T. Fernholz, *How to insure something that blows up once every twenty times you use it*, 10 September 2016, available online at:
https://qz.com/775481/how-to-insure-something-that-blows-up-once-every-twenty-times-you-use-it/.

[20] See AXA XL, above at 17.

[21] Interestingly enough, smaller fleets are generally more likely to carry in-orbit insurance because if something goes wrong than the small fleet operator is more likely to lose capability. A 2018 report from Aerospace Corporation's Rebecca Reesman states that 23% of commercial operators buy little to no on-orbit insurance.

[22] See Allianz.com, *Space Insurance*, available online at:
https://www.agcs.allianz.com/solutions/aviation-insurance/space-insurance.html#tabpar_1317_0Tab.

[23] For a comprehensive analysis of the current status of national legislations with regard to the space insurance market see B. Sandeepa Bhat, *Space Liability Insurance: Concerns and Way Forward*, Athens Journal of Law – Vol. 6, No. 1, January 2020, p. 40 et seq.

[24] R. Parker, *If hackers cripple your satellite, are you covered? Don't count on it.*, on SpaceNews.com, Sept. 18, 2019.

[25] G. Falco, *The Vacuum of Space Cybersecurity*, presented at the 2018 AIAA SPACE and Astronautics Forum and Exposition, 17-19 September 2018, Orlando, FL.

[26] N. Kshetri, *The Economics of Cyber-Insurance*, in IEEE IT Professional, Vol. 20, Issue 6, 2018, pp. 9-14.

[27] Ibid.

[28] Ibid.

[29] CyberInsureOne.com, *What is Cybersecurity Insurance*, available online at:
https://cyberinsureone.com/faq/what-is-cyber-security-insurance/.

[30] See N. Ksherti, above at 26.

[31] See R. Parker, at 4.

[32] Ibid.

[33] See N. Ksherti, above at 26.

[34] The subject of the case study uses the case of SpaceX's Starlink constellation as inspiration. The valuation of Starlink cannot be understated, with Morgan Stanley stating that SpaceX may be valued as an $175 billion company if Starlink is successful. While the constellation is most likely self insured, it is important to engage in this exercise to develop a standard for risk management due to the proliferation of satellites in the future.

[35] Aon Risk Solutions, *Insuring Space Activities*, October 2016, available online at: https://www.aon.com/russia/files/Insuring_Space_Activities_whitepaper.pdf.

[36] Ibid.

[37] Maochao Xu and others, *Cybersecurity Insurance: Modeling and Pricing*, North American Actuarial Journal, Vol. 23, Issue 2, pp. 220-249.

[38] The basis of a Monte Carlo simulation involves assigning multiple values to an uncertain variable to achieve multiple results and then to average the results to obtain an estimate.
For more on this see: https://www.investopedia.com/terms/m/montecarlosimulation.asp.

[39] See Maochao Xu and others, above at 37.
As this paper's entire scope focuses on the legal and policy aspects, it is worth noting that the authors posit a formula for a large scale network approximation.

[40] Ibid.

[41] Infection type can be classified as either infection outside the network or infection via the link (within the network).

[42] See Maochao Xu and others, above at 37.

[43] See N. Palkovitz, *Regulating a Revolution: Small Satellites and the Law of Outer Space*, Aerospace Law and Policy Series Volume 17, Kluwer Law International, 2019.
It is worth noting that at the time, the Dutch Space Act made TPLL insurance mandatory for Dutch satellite operators. However, it did not apply to small satellite activities.

[44] Ibid.

[45] Ibid.

[46] M. Sampson, *When Cyber Attacks Result in Physical Damage: Important Insurance Considerations*, published on law.com, 21 August 2020, available online at: https://www.law.com/thelegalintelligencer/2020/08/21/when-cyber-attacks-result-in-physical-damage-important-insurance-considerations/?slreturn=20200902172653.

[47] See R. Parker, above at 24.