CHARLES UNIVERSITY

Cybersecurity for Outer Space – A Transatlantic Study

MAY 2018

UofG: 2272775

CU: 76213115

Presented in partial fulfilment of the requirement for the Degree of MSc International Security, Intelligence and Strategic Studies (SECINTEL)

Word Count: 19,922

Supervisor UofG: Adrian Florea

Supervisor Charles Uni: Bohumil Doboš

Table of content

Abstract

Cyber attacks can target any nodes of the space infrastructure, and while these attacks are called non-violent, there is a credible capability to use cyber attacks to cause direct or indirect physical damage, injury or death. However, the vulnerability of satellites and other space assets to cyber attack is often overlooked, which is a significant failing given society's substantial and ever increasing reliance on satellite technologies. Through a policy analysis, this dissertation assess the set of political provisions provided by the European Union to address the cyber security issue of the space infrastructure.

Such study aims at exploring the geopolitical consequences linked to space cyber security risks, and at assessing the political preparedness of the European Union to address these challenges. The perspective of transatlantic cooperation to further support both American and European effort to tackle this security risk is also addressed. The overarching value of the study is to contribute to future European cyber security for space and transatlantic debates by providing useful perspectives and key takeaways on these two domains.

Ultimately, he existing set of policies are not sufficient to address the cyber security issue in Outer Space, a unified approach by the European Union and the United States could improve information-sharing and the capacity to respond quickly attacks, strengthening cybersecurity across Europe, and throughout the international scene.

Keywords: space security, cyber attacks, European Union, United States, transatlantic, policy analysis, NIS Directive, Cyber Diplomatic Toolbox, NIST Cybersecurity Framework, human security.

Acknowledgement

I would like to thank my supervisors from Charles University, Bohumil Dobos, and from Glasgow University, Adrian Florea, for their patience and help throughout this process.

I would also thank Jana Robinson, Director of the Space Security Program at the Prague Institute for Security Studies (PSSI), for offering me an internship during the Summer, and for her helpfulness.

Finally, I would like to thank the Director and all the staff working at the European Space Policy Institute (ESPI), for their kindness and trust.

-- To Arthur.

I. Introduction

The European economy, society and security depends heavily on the space infrastructure. This ever-growing use of space-based data and services by a variety of public and private actors creates a virtually invisible dependence on space technologies, which closely relates to the cyber domain. The growing importance of the space infrastructure for European security raises new stakes, such as its protection from harm. Yet, the growing threat posed by cyber-attacks is often misunderstood and lost in the wider debate of security.

This chapter introduces the issue of cyber security risk on space system and develop the rationale behind the study.

1.1 Background

European satellites directly supports public actions to address economic, societal, environmental, and security issues at a national and international level.[1] Moreover, most of the critical infrastructures — e.g energy, finance, defence, communications, healthcare, agriculture — rely on space systems for their operation.[2] This ever-growing satellites' contribution to the protection of people while promoting peace and assuring sustainable continuous development, makes space infrastructure a vital component of the 'human security' framework.[3] As the use of space applications becomes more pervasive, brings more benefits, and becomes part of the business-as-usual routine, the dependence on the space infrastructure creates new vulnerabilities for economy,[4] and society at large. Thus, if satellites were to be disabled or disrupted in any way, it would have a rippling

[1] Jakhu, R. & Pelton, J. (2017). 'Introduction to the Study on Global Space Governance', *Global Space Governance: An International Study*, (Eds Ram S. Jakhu).
[2] Department of Homeland Security (DHS), (2018). 'Critical infrastructure sectors' on the *Department of Homeland Security of the United States, [*https://www.dhs.gov/critical-infrastructure-sectors]. (Accessed February 12, 2018).
[3] Sheehan M. (2015). 'Defining Space Security', *Handbook of Space Security*, (Springer, New York, NY).

[4] It was estimated that a (theoretical) incapacitation of space assets would lead to a net economic loss around EUR 50 billion per year, and put up to 1 Million jobs at risk (European Commission, 2018).

effect on the critical infrastructure it enables, affecting public safety, and national security, and experiencing loss of lives.[5]

Therefore, the growing importance of the space infrastructure for European security raises new stakes, such as its protection from harm. European space-faring nations have thus, to deal with a growing challenge to the security of their space infrastructure: the development of cyber attacks,[6] i.e. 'cyber operation, weather offensive or defensive that is reasonably expected to cause injury or death to persons or damage or destruction to objects'.[7] Space operations are entirely cyber dependant,[8] and critical portion of cyberspace can only be provided by space operations.[9] As the space and cyberspace domains are also linked operationally for the military,[10] cyber-related vulnerabilities of space assets are a major concern for national security.[11] This raising issue is part of the 'space security' literature and more specifically the importance to protect space assets and systems against threats to ensure a sustainable operation of space activities, is referred as *Security in Outer Space* in the litterature.[12]

1.2 Research Focus

Cyber attacks will probably account for the most preferred offensive strategies when the objective will be to disrupt an entire space system.[13] The unprecedented level of threat is driven by increasingly sophisticated cyber-attacks from a growing number of cyber-capable entities. The identification of threat actors can be limited to three main

---

[5] Grisham, P. (2017). 'Satellite Cybersecurity and Information Assurance: How Secure Are Our Nation's Satellites?', *Keynotes from CompTIA webinar,* (March 1, 2017).
[6] European Commission (2017). 'Building an Effective European Cyber Shield', *Strategic Notes*, (Issue 24, 8 May 2017).
[7] Schmitt, et al. (2013). T*allinn Manual on the International Law Applicable to Cyber Warfare*. NATO CCDCOE. (Cambridge University Press: 2013).

[8] Robinson, J. (2016). "Governance challenges at the intersection of space and cyber security". *The Space Review, (*February 15, 2016).
[9] Joint Chiefs of Staff, (2013). 'Cyberspace Operations', *Joint Publication (JP) 3-12 (R)*, *Cyberspace Operations*, (5 February 2013, v-vi and I-2).
[10] Gini, A. (2014). 'Cyber Crime - From Cyber Space to Outer Space', *Space Safety Magazine*, (February 14, 2014).
[11] Robinson, J. (2016). 'Governance challenges at the intersection of space and cyber security'. *The Space Review*, (February 15, 2016).
[12] Mayence J-F (2010). 'Space security: transatlantic approach to space governance', *Prospects for transparency and confidence-building measures in space.* (ESPI, Vienna, p 35).

[13] Pasco, X. (2015). "Various Threats of Space Systems", *Handbook of Space Security, (Springer Science+Business Media* New York, p.674).

categories of actors:[14] profit-driven criminals; ideologically motivated hackers or extremists, and nation-states. The anonymity offered by cyber-attacks is important for any malicious operations to hack satellites in order to compromise foreign networks, or cover illegal activities.[15] Indeed, unlike a missile, traveling from one determinable geographic location to another through physical airspace, cyberattacks can travel internationally through cyberspace in moments, implicating computers in countries far from the original location of the hacker.[16]

Therefore, foreign and non-state actors are increasingly attempting to exploit, penetrate and disrupt satellite infrastructure. The threat posed by Nation-States attacks is particularly interesting to address, as not only the disruption of capabilities that space assets provide would have immediate, far-reaching and devastating economic and social repercussions, it would also have political and geo-strategic consequences.[17] Yet, no mapping and affective deterrent structures exist addressing space cyber risks and attacks, i.e. via established norms, active dissuasion, or accountability and enforcement measures.

Therefore, securing the European space infrastructures — ie. the entire system comprising the physical satellite, data uplink and downlink systems, ground stations — is a key area of space policy development.[18] However, the specific cyber security risk at the crossroad of Outer Space have not been fully grasped by the various European space stakeholders, and remain largely unaddressed.[19] Thus, policies and investments have been lacking, leaving the European space assets at risk.[20] In this regard, the Chatham House reported in 2016 that:

> 'The vulnerability of satellites and other space assets to cyberattack is often overlooked in wider discussions of cyber threats to critical national infrastructure.

[14] Clapper, J. (2015). *Worldwide Threat Assessment of the US Intelligence Community* – Statement for the Record. Senate Armed Services Committee, (February 26, 2015).

[15] Tanase, S. (2015). 'Satellite Turla: APT Command and Control in the Sky', *Kaspersky Lab*, (Sept. 9, 2015).

[16] Landler, M. & Markoff, J. (2007). "Digital Fears Emerge After Data Siege in Estonia", The *New York Times*, (May 29, 2007).

[17] Robinson, J. (2016). 'Governance challenges at the intersection of space and cyber security'. *The Space Review*, (February 15, 2016).

[18] European Commission (EC) (2016). *Space Strategy for Europe.* COM(2016) 705 final, (26 October 2016).

[19] *Ibid.*

[20] European Commission (2016). '*Fact Sheet: FAQ: Joint Framework on countering hybrid threats*', (6 April 2016).

This is a significant failing, given society's substantial and ever increasing reliance on satellite technologies for navigation, communications, remote sensing, monitoring and the myriad associated applications'.[21]

Therefore, against the cyber threat, Europe requires improved cooperation, clear strategy frameworks, and the effective use of available tools. Failing to address the vulnerabilities at the junction of space-based or space-derived capability with cybersecurity could cause major national, regional and international security concerns.[22]

1.3 Overall Research Aim and Individual Research

The deteriorating situation of security in space has been acknowledged by the European Union (EU), who made of "ensuring the protection and resilience of critical European space infrastructure" a flagship objective of the Space Strategy for Europe.[23] However, if the European Union recognised the importance of cybersecurity through its publication of the EU Cyber Security Strategy in February 2013,[24] which was followed by the Network and Information Security (NIS) Directive in 2016.[25]

However, whether norms and regulation will be developed to ensure the adoption of cyber best-practice for Outer Space remains to be seen. The risk posed by a lack of governance at the European level, is that without establishing a comprehensive standard, it becomes difficult to track European-wide efforts to address threats to space systems.

Therefore, if European Union has issued a set of policies intended to address the cyber threat, more study is required to understand how these political provisions can apply to the space domain. The issue of good governance to address the cyber threat against space assets is double: 1) it is to provide an opportunity to share remediation strategies and information on the attacker, which could prevent other organisations from suffering the same fate;[26] and 2) it is to provide clear procedures to deal with escalatory

[21] Livingstone, D. & Lewis, P. (2016). 'Space, the Final Frontier for Cybersecurity?', *Chatham House Research Paper*, p.2.
[22] UK HM Government (2014), National Space Security Policy, (UKSA/13/1292).
[23] European Commission (EC) (2016). *Space Strategy for Europe.* COM(2016) 705 final, (26 October 2016).
[24] European Union for Foreign Affairs and Security, (2013). The Cybersecurity Strategy of the European Union – An Open, Safe and Secure Cyberspace. JointCOM(2013) 1 Final. (Brussel, February 7, 2013).
[25] European Parliament, (2016). *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*. (Brussels, July 2016).
[26] Bardin, J. (2014). "Satellite Cyber Attack Search", *Cyber Security and IT Infrastructure Protection*, (Elsevier Inc, p.317).

spirals and other eventualities, with substantial penalties for violators.[27] Thus, to address efficiently the issue, the EU has to develop policies that: 1) foster trusted information sharing on security threats, risks and incidents amongst the Member States and between the private and the public sector; and 2) back governments to conduct evidence-based policy making and to respond to incidents affecting governments' networks in a timely manner.[28]

Moreover, due to the borderless nature of space, fostering an information-sharing cybersecurity framework would be best done at an international level; this arrangement should be managed initially by an international 'community of the willing' – a limited number of able states and other critical stakeholders within the international space supply chain and insurance industry.[29]

Therefore, in its strategy, the European Union clearly states its intention to continue its effort to develop international cooperation in the field of space security.[30] The EU and points the United States (U.S.) as a key partner,[31] as space has always held a prominent defence and national dimension for the U.S., and securing their space assets a strategic priority.[32] The U.S. approach to space security underlines the importance of cooperation, or at least coordination, to tackle challenges to space infrastructures security.[33] Notwithstanding, building an effective transatlantic partnership benefiting equally to both partners requires preliminary steps, including a shared assessment of space security challenges, a common understanding of partners' priorities, insights on respective approaches to the issue, and a sound evaluation of drivers and obstacles to cooperation.

Therefore, the goal of the study is to characterise and analyse approaches to space cybersecurity by the European Union, and asks the following question: "How can the current cybersecurity policies of the European Union and the transatlantic partnership

---

[27] Robinson, J. (2016). 'Governance challenges at the intersection of space and cyber security'. *The Space Review*, (February 15, 2016).
[28] As laid out by the European Commission. (2013). "Impact assessment", Proposal for a Directive of the European Parliament and of the Council *Concerning measures to ensure a high level of network and information security across the Union.* (SWD(2013) 32 final, p.25).
[29] Livingstone, D. & Lewis, P. (2016). 'Space, the Final Frontier for Cybersecurity?', *Chatham House Research Paper.*
[30] European Commission (EC) (2016). *Space Strategy for Europe.* COM(2016) 705 final, (26 October 2016).
[31] *Ibid.*
[32] Kaufman, M. (2006). 'Bush Sets Defense As Space Priority'. *The Washington Post*, (October 18, 2006).
[33] Government of the United States (2010). *National Space Policy of the United States of America*.

with the United States improve space governance while addressing the issue of cyber attacks in Outer space?". The dissertation will thus address in priority the European Union and U.S. approaches to space cybersecurity and will focus essentially on key areas for transatlantic development. Thus, the goal study characterise and analyse approaches to space systems cybersecurity by the European stockholders and the United States, and discuss potential transatlantic cooperation in the field of space cybersecurity.

The objective of this dissertation is three-fold. First, it analyses the critical nature of cybersecurity for European space infrastructures, and assess threats from cyber attacks to this infrastructure. Second, it analyses the main security policies consideration to cybersecurity for EU's current and future space systems. Third, it offers a number of ideas for improving European cybersecurity with respect to space security through the transatlantic cooperation. The dissertation is focusing more on the European Union but acknowledges that, despite the emergence of the EU as a security and space actor, member states must continue to play essential roles in steering common policies, furthering European space activities and leading technological development.

1.4 Outline Research Methods

The first part of the research is to identify the cybersecurity policies space systems need. Therefore, the research will analyse the literature in order to compile and synthesise the different suggestions made by academics of various fields. This step will not only formulate the cybersecurity recommendations for space systems, it will also present a useful framework for analysis. Thus, the second part of the research will be to evaluate the cybersecurity policies developed by the United States on one hand, and by the European Union on the other one.

Therefore, the research method used is the policy analysis, which will determine the differences, pros, cons, and gaps of each policy models used on either side of the Atlantic. Following the policy analysis, the third part of the research will explore where and how the U.S and EU could cooperate on the topic of cybersecurity for space systems. This step will be an important part of the dissertation as it can support or

dismiss the argument that a transatlantic cooperation would be beneficial and required in order to get a better protection for space systems against cyberattacks.

This is a study on the development of space governance by European actors to address the threat of cyber-attacks through a space-cyber framework in order to bring better space security at an international level. This dissertation will explore further new concepts of space governance, and will do so by investigating the management of space cybersecurity in Europe. The dissertation is intended primarily for a scholarly audience (particularly students and analysts in the fields of space policy and security studies), but it also may hope to reach interested members of the policymaking community, the European space community, and the general public.

Therefore, the research is based primarily on the collection and compilation of public information on the topic. The report begins by describing the transatlantic "cybersecurity commons" and the strong space security ties that dictate a shared approach to cybersecurity. It then reviews the relevant public policy landscape in the EU and the United States. At the EU level, this consists primarily of the existing set of two policies: the Network Information Security Directive (NIS Directive),[34] and the European Cybersecurity Toolbox.[35] In the United States, the centrepiece is the National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (NIST Framework).[36]

1.5 Value of the Research

Therefore, the research aim to raise awareness on the topic of cybersecurity, but most importantly on space security. Contribute further to the research on space security and transatlantic security cooperation. Indeed, the topic provides an excellent opportunity to address and develop transatlantic relations in space and to support a transatlantic space policy study. Such study aims at endorsing a common understanding of space cybersecurity challenges and of the way of a reinforced transatlantic cooperation can

[34] European Parliament, (2016). *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*. (Brussels, July 2016).
[35] Council of the European Union, (2017). *Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox")*. (Brussels, 7 June 2017).
[36] National Institute of Standards and Technology (2018). *Cybersecurity Framework: Revised Version 1.1*, (April 16, 2018).

further support both American and European effort to tackle these challenges. The overarching value of the study is to contribute to future European security and transatlantic debates in space by providing useful perspectives and key takeaways on these two domains.

II. Literature Review

The goal of the study is thus to characterise and analyse approaches to space cybersecurity by the European Union and the United States, and discuss potential transatlantic cooperation in the field of space cybersecurity.

To help in this endeavour, this chapter lays out what research has been done by others on these issues. The literature gives first introduce previous research done on the broader topic of space security; then the chapter highlights the cybersecurity issue for space systems; and finally, the chapter highlights emerging issues and gap for research that called for this study.

2.1 Defining space security

Security is, in general terms, about being free from danger or threat. In practical terms, this means freedom from doubt, anxiety, or fear based on well-founded confidence that there are mechanisms and processes in place to ensure security as a condition.[37] However, attempts to pin down exactly what is encompassed by the word security prove to be elusive as there is no single universally accepted definition of the concept of 'security.' Similarly, 'space security' is a well discussed issue in literature, but rarely defined.

Traditionally space security was primarily defined in bipolar terms as part of the strategic balance between the United States and the Soviet Union, and was focused on military and environmental aspects of accessing and using space.[38] Then, space security was defined by the Space Security Index as the secure and sustainable access to, and use of, space and freedom from space-based threats.[39] This definition encompasses the security of the unique outer space environment, which includes the physical and operational integrity of man-made assets in space and their ground stations, as well as

[37] Martinez, P. (2015). 'Space Sustainability', *Handbook of Space Security*. (Springer Science+Business Media New York).
[38] Hays, P. (2015). "Defining Space Security ", *Handbook of Space Security*. (Springer Science+Business Media New York, p.3-7).

[39] Space Security Index (2017). *Space Security Index 2017*, (Eds. Jessica West, Ontario: May 2017).

security on Earth from threats originating in space.[40] However, Michael Sheehan explains that this definition, in order to be comprehensive, can be further expanded to include the crucial role played by space systems to support defence and security activities on Earth.

Therefore, a different definition including a broader perspective on security that emphasises the use of space for security and defence, the security of assets in space against natural and man-made threats, as well as security from threats originating in space is preferred.[41] From a broader perspective, considering all the aspects of space and its relation to human security, the study thinks that the three-dimensional approach as defined by Mayence actually address all these aspects: *outer space for security,*[42] i.e. the use of space systems for security and defence purposes, *security in outer space,* i.e. how to protect space assets and systems against natural and/or human threats or risks and ensure a sustainable development of space activities, and *security from outer space,* i.e. how to protect human life and Earth's environment against natural threats and risks from outer space.

Therefore, Martinez insist that space security is sometimes perceived to be predominantly the preoccupation of the advanced space actors and thus far removed from the day-to-day concerns of the non-space nations.[43] However, others (particularly emerging or aspiring space nations) may see the promotion of multilateral space security discussions as an attempt by the leading space actors to advance and preserve their national space interests while erecting entry barriers to aspiring newcomers on the pretext that the space environment is already "saturated" with actors. Neither of these perceptions helps to build multilateral consensus on normative rules of behavior for all space actors.

Therefore, we need to include governance and theoretical issues as other foundational aspects of space security. Effective governance is needed for humanity to derive more benefits from space; space governance also seeks to ensure space is used in stable and sustainable ways. Therefore, space security is viewed as an issue of

---

[40] Space Security Index (2013). *Space Security Index 2013*, (Eds.Cesar Jaramillo, Ontario: June 2013).
[41] Sheehan, M. (2015). "Defining Space Security ", *Handbook of Space Security*. (Springer Science+Business Media New York, p.17-18).
[42] Mayence J-F (2010). 'Space security: transatlantic approach to space governance', *Prospects for transparency and confidence-building measures in space*. (ESPI, Vienna, p 35).
[43] Martinez, P. (2015). 'Space Sustainability', *Handbook of Space Security*. (Springer Science+Business Media New York).

international development and cooperation between states,[44] which demands effective governance to ensure space is used in stable and sustainable ways through multilateral cooperation.[45] Greater reliance on outer space means that regional and international cooperation are becoming inevitable.

2.2 Governance and cooperation issues in space security

Sheehan explained that cooperation that is unregulated in nature could further insecurities at multiple levels.[46] The governance of space is not only about the post-modern non-territorial governance in outer space, but also about very traditional territorial governance of space technologies, which Suzuki explain eventually lead to the governance of geopolitical issues.[47] Moreover, international relations are characterised by the lack of a clearly defined systemic order, and there is now no easy-to-be-found description available indicating whether a general model for global security can be defined.[48]

Therefore, international governance is not easily achievable. Eligar Sadeh identifies two key obstacles to more enlightened space governance: difficulties in attaining collective action in relation to the commons of space and problems with developing shared understanding about strategic stability and advancing strategic assurance for sustainable uses of space as a shared strategic goal.[49] Similar to Sadeh, Max Mutschler's describes how international relations theory can be used to explain various patterns of security cooperation in space and illuminates why there have been only limited successes thus far in achieving space security cooperation:[50] Neorealism explains this lack of cooperation with the difficulties to achieve balanced gains; neo-institutionalism sees the

[44] Sheehan, M. (2009). *Securing Outer Space*, (Routledge: NY).
[45] Harrison, R. (2013). 'Unpacking the Three C's: Congested, Competitive, and Contested Space', *Astropolitics* (11(3):123-131, September 2013).
[46] Rajagopalan, R. (2016). "The International Code of Conduct and Space Sustainability", *Yearbook on Space Policy 2014.* (C. Al-Ekabi et al. (eds.), Springer-Verlag Wien, p.232).
[47] Suzuki, K. (2016). "How Governance Models Affect Geopolitics: The Asian Case Study", *Yearbook on Space Policy 2014.* (C. Al-Ekabi et al. (eds.), Springer-Verlag Wien, p.200).
[48] Algieri, F. and Kammel, A. (2010). 'Anmerkungen zum ersten Jahrzehnt der ESVP' *Strategie und Sicherheit,* (Volume 2010, Issue 1, Pages 61–72).
[49] Sadeh, E. (2015). "Obstacles to International Space Governance", *Handbook of Space Security*. Springer (K.-U. Schrogl et al. (eds.), Science+Business Media New York, p.24).
[50] Mutschler, M. (2015). 'Security Cooperation in Space and International Relations Theory', *Handbook of Space Security*. (K.-U. Schrogl et al. (eds.), Springer Science+Business Media New York).

establishment of effective rules and mechanisms to verify the compliance of states as a main hurdle; and from a Constructivist/Liberal perspective the main problem lies in the dominant beliefs about the value of unilateral space policies.

Therefore, neorealism, which is based on the seminal work of Kenneth N. Waltz, established a systemic theory of international relations, which draws conclusions about the behaviour of the units of the system –states – from the structure of the system.[51] The defining feature of this structure is anarchy. The anarchical structure produces a self-help system in which every state is responsible for its own security, simply because there is no institution at the international level and thus above the state that could ensure security.[52] The internal characteristics of the units, for example, the respective political systems of the states, are treated as irrelevant for the explanation of international politics; states are seen as unitary actors that differ only with regard to their "capabilities" – their power, usually measured in terms of military and economic indicators. As "like units," all states share the central goal of survival, which in an anarchical environment means that states are compelled to maximise their security. Power and the power position of a state are of crucial importance in this regard.[53]

Therefore, according to neorealist accounts, the unequal distribution of gains is a central obstacle to international cooperation. In an international system characterised by anarchy, states cannot tolerate relative losses in comparison with their rivals as described by Waltz,[54] and shared by Grieco.[55] This holds true in particular with regard to arms control agreements that seek to limit or ban whole categories of weapons. If there are different levels of technological development with regard to the weapon technology, the states with lesser capability would naturally gain more from an arms control agreement than those states that have the technological edge. This is the case with regard to space weapon technology, too.[56]

---

[51] Waltz K. (1959). *Man, the state and war*. (Columbia University Press, New York); and Waltz K. (1979). *Theory of international politics*. (Random House, New York).
[52] *Ibid.*
[53] Mutschler, M. (2015). 'Security Cooperation in Space and International Relations Theory', *Handbook of Space Security*. (K.-U. Schrogl et al. (eds.), Springer Science+Business Media New York).
[54] Waltz, K. (1979). *Theory of international politics*. (Random House, New York).
[55] Grieco J. (1988). *Anarchy and the limits of cooperation - A realist critique of the newest liberal institutionalism*. (Int Organ 42:485–507).
[56] Mutschler, M. (2015). 'Security Cooperation in Space and International Relations Theory', *Handbook of Space Security*. (K.-U. Schrogl et al. (eds.), Springer Science+Business Media New York).

However, while neorealism can explain the lack of formal security cooperation, it has more difficulties explaining the fact that we have seen a more tacit form of security cooperation in space between the two superpowers of the Cold War for example.[57] Neo-institutionalists like Robert Keohane are much more optimistic with regard to international cooperation.[58] While they acknowledge the anarchical structure of the international system, they argue that there is a high degree of interdependence between states which creates strong incentives to cooperate in order to maximise their utility. In an interdependent world, states have many mutual interests. Zero-sum games are the exception, not the rule. However, these mutual interests do not automatically lead to international cooperation.[59]

Therefore, constructivist accounts of international relations criticise rationalist approaches like neorealism and neo-institutionalism for treating states' identities and interests as exogenously given and thereby "blackboxing" the processes that lead to those identities and interests.[60] In consequence, rationalist approaches are seen as incomplete because they cannot account for changes of the actors' interests that are independent of material factors. Thus, according to constructivists, the demand for cooperation – whether in the security field or elsewhere – depends on the actors' perception of the problems at hand. Goldstein and Keohane think these perceptions, in turn, are a product of the causal and normative beliefs of the actors,[61] idea shared by Hasenclever and his coauthors.[62]

Therefore, various constructivist authors acknowledge that "ideas do not float freely".[63] Ideas and beliefs need agents that carry them, and these agents have to act

---

[57] *Ibid.*
[58] Keohane R. (1984). *After hegemony. Cooperation and discord in the world political economy*. (Princeton University Press, Princeton); and Keohane R. (1989). *Neoliberal institutionalism. A perspective on world politics*. In: Keohane R. (ed) International institutions and state power. Essays in international relations theory. (Westview Press, Boulder, pp 1–20).
[59] Mutschler, M. (2015). 'Security Cooperation in Space and International Relations Theory', *Handbook of Space Security*. (K.-U. Schrogl et al. (eds.), Springer Science+Business Media New York).
[60] Mutschler, M. (2015). 'Security Cooperation in Space and International Relations Theory', *Handbook of Space Security*. (K.-U. Schrogl et al. (eds.), Springer Science+Business Media New York).
[61] Goldstein J, and Keohane R. (1993). *Ideas and foreign policy. Beliefs, institutions, and political change*. (Cornell University Press, Ithaca).
[62] Hasenclever A., Mayer P., and Rittberger V. (2002). *Theories of international regimes*. (Cambridge University Press, Cambridge).
[63] Risse-Kappen T. (1994). *Ideas do not float freely - Transnational coalitions, domestic structures, and the end of the cold war*. (Int Organ 48:185–214).

within power structures and lobby for their ideas to get politically selected. This reference to domestic structures and actor coalitions connects the debate about the role of knowledge and ideas with what can be seen as one strand of the liberal school of thought in international relations, according to which international politics are dependent on the constellation of the societal structures and interests of states. For those liberal authors, of whom Andrew Moravcsik is probably the most renowned, states are seen as transmission belts for the dominant societal preferences, as they are represented by various interest groups.[64] This constructivist/liberal account would explain the limited security cooperation in space by recurring to the dominant beliefs about the value of unilateral behaviour if compared with security cooperation in space.[65]

2.3 Drive and Barriers for developing Space Cybersecurity governance

Markus Hesse and Marcus Hornung find that too often critical space infrastructure is overlooked.[66] For example, Global Positioning System timing signals currently provide the "heartbeat" that synchronises all global telecommunications networks, yet there is a lack of appreciation for this dependency and underdeveloped policies to ensure protection of this critical space infrastructure. As space infrastructure grows in importance, it is imperative that the United States, European Union, and others find better ways to develop these needed policies. Space safety is necessary for the sustainable development of space yet, as Joe Pelton and his coauthors describe, safety considerations are too often an afterthought for space security issues.[67]

Therefore, for Suzuki space security calls for good space governance in order to protect and maintain the sustainability of the space environment.[68] Global governance is made up of legal mechanisms (e.g., norms, rules, and institutions), put in place through political processes and entities, that affect peace and security, and social and economic

[64] Moravcsik A. (1997). *Taking preferences seriously - A liberal theory of international politics*. (IntOrgan 51:513–553).
[65] Mutschler, M. (2015). 'Security Cooperation in Space and International Relations Theory', *Handbook of Space Security*. (K.-U. Schrogl et al. (eds.), Springer Science+Business Media New York).
[66] Hesse, M. and Hornung, M (2015). 'Space as a Critical Infrastructure', *Handbook of Space Security*. (K.-U. Schrogl et al. (eds.), Springer Science+Business Media New York).
[67] Pelton, J. et al. (2015). 'Space Safety', *Handbook of Space Security*. (K.-U. Schrogl et al. (eds.), Springer Science+Business Media New York).
[68] Suzuki, K. (2016). 'How Governance Models Affect Geopolitics: The Asian Case Study', *Yearbook on Space Policy 2014*. (C. Al-Ekabi et al. (eds.), Springer-Verlag Wien, p.199).

development.[69] The existing international regime for space, the rules and norms, were originally formulated in the 1960s and 1970s. They were embodied in five international treaties related to space, with its core the 1967 Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space.

Therefore, since, the global governance of space activities has been maintained mainly through United Nations (UN) treaties, as well as through several non-binding guidelines and transparency and confidence-building measures, or TCBMs.[70] However, the current global governance system for space security is inadequate and in need of improvement. Although the Outer Space Treaty Article IV prohibits the placement of nuclear weapons or other weapons of mass destruction in orbit around Earth, the treaty does not outlaw many of the potential weapons capabilities or means of warfare such as lasers, or cyber-attacks against space systems.[71]

Moreover, the space domain is considered a global commons in that the domain lies beyond the sovereign jurisdiction of states, is governed by international law, and is available for all actors to access and use. For Gallager, the Global Commons logic seeks more informal cooperation so that a multitude of self-interested space users can share a ‘‘congested’’ environment without causing unintentional harm.[72] However, Hardin already described that a commons that is unregulated (i.e., no governance) can result in a “tragedy of the commons”.[73] This situation is rooted, for instance, in rational self-interested state behaviour regarding the commons. The tragedy for Sadeh is a function of damage to the commons caused by free access and free use, like the possibility of interference and attacks on space assets.[74]

Therefore, to mitigate these tragedies, collective action is necessary. However, the lack or inadequacy of national policy documents in the cyber and space spheres creates opacity concerning state objectives, which in turn fosters ‘ambiguity of intent’ surrounding state actions and renders states more likely to construe other states’ actions

[69] Jakhu, R. & Pelton, J. (2017). "Introduction to the Study on Global Space Governance", *Global Space Governance: An International Study*, (Eds Ram S. Jakhu, p.16).
[70] Pellegrino, M., & Stang, G. (2016). *Space security for Europe. (*Paris: European Union Institute for Security Studies).
[71] Baseley-Walker, B. (2014). "The UN Structure: The Intersection of Cyber Security and Outer Space Security", in *Chatham House*, (December 2014, p.48).
[72] Gallagher, N. (2010). "Space Governance and International Cooperation", *Astropolitics, 8:2-3*.
[73] Hardin, G. (1968). ‘The Tragedy of the Commons’, Science, (13 Dec 1968: Vol. 162, Issue 3859, pp. 1243-1248).
[74] Sadeh, E. (2015). "Obstacles to International Space Governance", *Handbook of Space Security,* (K.-U. Schrogl et al. (eds.),. Springer Science+Business Media New York, p.24).

as offensive. In her paper on space cybersecurity, Baylon noted that the absence of such documents also hinders dialogue, reducing prospects for international cooperation.[75]

Therefore, the lack of coordination between these stakeholders and stakeholders at other levels (European and national) brings major discrepancies in the way space security is addressed. The current situation implies a significant risk of inadequate coordination which could lead to inefficiencies such as governance gaps and overlaps. the effectiveness of the implementation of coordinated European actions will depend on the ability to achieve maximum synergy within a coherent European effort among intergovernmental and communitarian actors but also with national actors, who remain the main players in this field.[76] At the European level, the current fragmentation existing in space policies makes it difficult to enforce legal requirements ensuring minimum cyber security protection.

2.4 Way Forward for a Space Cybersecurity Framework

Responsive space is a recent catchphrase referring to aspirations for space capabilities to support a wide range of mission areas in flexible ways, become more affordable, and be developed and employed more quickly. Nina-Louisa Remuss explores security-related dimensions of responsive space and examines how the well-known approach developed by the US Department of Defense can inform a European path toward improving responsive space capabilities.[77] Dario Sgobbi and his coauthors examine the strong interrelationships between space and cyber security. Although many aspects of space and, especially, cyber security must be far better developed, the authors assert that using systems engineering concepts and methodologies is key to tackling challenges in both these fields simultaneously and to achieving space systems that are truly cyber secure.[78]

The proliferation of threats such as these to governments, individuals, and businesses large and small coming from independent actors and nation-states has

[75] Baylon, C. (2014). "Challenges at the Intersection of Cyber Security and Space Security: Country and International Institution Perspectives", *Chatham House*, (December 2014, p.2).
[76] Naja, G & Mathieu, C. (2015). "Space and Security in Europe", *Handbook of Space Security,* (K.-U. Schrogl et al. (eds.),. Springer Science +Business Media New York, p.377).
[77] Remuss, N. (2015). Responsive Space', *Handbook of Space Security,* (K.-U. Schrogl et al. (eds.),. Springer Science +Business Media New York).
[78] Sgobbi, D. et al. (2015). 'Space and Cyber Security', *Handbook of Space Security,* (K.-U. Schrogl et al. (eds.),. Springer Science +Business Media New York).

increased the need for a common response. One way to prevent threats to space assets is to persuade potential aggressors that any benefits from interference are outweighed by expected costs. This is the overall basis for deterrence as discussed by Harrison.[79] The concept of deterrence can be applied to think about how to overcome the obstacle of protection of space assets from threats as a shared strategic goal. However, the question of concern for deterrence is whether these mechanisms have deterrent effects that are shared and mutual among those that abide by the norms.

Therefore, crafting an international strategy will require agreeing to certain constraints on national sovereignty with the assumption of greater individual and collective gains. To date, such agreements have been difficult—but not impossible—to establish as noted Moltz.[80] It is thus recommended to align international, regional and national policies on space cyber security requirements. Baylon thus recommend a platform for further consultation and coordination on space cyber security, lead by the European Commission and with the support of the Member States is desirable at this level.[81]

Therefore, several papers and articles advocates a risk management approach and is in line with the NIST Cybersecurity Framework. Communications and transmission security measures are employed using standards such as those defined by the National Institutes of Standards and Technology (NIST).[82] What's interesting about the updates to the framework is that it provides new details on managing cyber supply chain risks and this might be one of the most important components in dealing with cyber threats affecting satellites.[83]

Therefore, there is, for Livingstone and Lewis an urgent requirement to develop a space cybersecurity regime that will inform and organise policy efforts and subordinate strategies, while remaining federally networked rather than controlled from a centre or

[79] Harrison R., el al. (2009). *Space deterrence: the delicate balance of risk*.
[80] Moltz, J. (2010) "Space and Strategy: A Conceptual versus Policy Analysis", *Astropolitics, 8:2-3*.
[81] Baylon, C. (2014). "Challenges at the Intersection of Cyber Security and Space Security: Country and International Institution Perspectives", *Chatham House*, (December 2014).
[82] Bardin, J. (2014). "Satellite Cyber Attack Search", *Cyber Security and IT Infrastructure Protection*, Elsevier Inc, p.320.
[83] Grisham, P. (2017). "Satellite Cybersecurity and Information Assurance: How Secure Are Our Nation's Satellites?", *Keynotes from CompTIA webinar,* March 1, 2017.

hierarchically driven.[84] Thus, there needs to be more study in which of available cybersecurity guidelines are applicable to space, and this is what this dissertation will explore the new cybersecurity guidelines for the space domain.

Therefore, the aim of the dissertation is to capture the concept of cyber threats to space infrastructure (i.e. cyber operation, weather offensive or defensive that is reasonably expected to cause injury or death to persons or damage or destruction to objects),[85] as well as to assess the level of awareness and preparedness in Europe on the policy level with regard to these threats.

[84] Livingstone, D. & Lewis, P. (2016). "Space, the Final Frontier for Cybersecurity? ", *Chatham House Research Paper*, p.24.
[85] Schmitt, et al. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. NATO CCDCOE. (Cambridge University Press: 2013).

III. Methodology

The study asks the following: "How can the current cybersecurity policies of the European Union and the transatlantic partnership with the United States improve space governance while addressing the issue of cyber attacks in Outer space?". To address the issue of cybersecurity for space systems, the study is looking at the set of policies available to European space stakeholders, which will be analysed and compared to the U.S. approach to cybersecurity.

To do so, this chapter first gives essential definitions and concepts which are used throughout the paper; then, the chapter will present the scope of the study, which focuses on the European Union and the United States; and finally, the research method of policy analysis will be detailed.

The objectives of the study can be understood as follow:

1. Evaluate the European cybersecurity policies applicable to the space domain; and

2. Explore transatlantic cooperation perspective on the issue of space cybersecurity.

3.1 Definitions

In order to structure the analysis conducted in this study and to provide clear definitions of concepts used throughout the report, an introductory examination of generic risk management and dependability models was performed. Indeed, to fully understand space security - what it entails and how it can be enhanced - key concepts, inherently intertwined, must be distinguished.

3.1.1 Space security

In this report, ‘Space Security’ is understood primarily as ‘Security in Outer Space’ referring to the protection of the space infrastructure from threats so that this

infrastructure can fulfil its specific functions as expected. The topics of 'Outer Space for Security' (i.e. the use of space-based capabilities to support security and defence activities) and of 'Security from Outer Space' (i.e. the protection of the Earth against space-based threats) are not addressed directly in this study.

Security in Outer Space	Outer Space for Security	Security from Outer Space
The protection of the space infrastructure against natural and man-made threats or risks, ensuring the sustainability of space activities.	The use of space systems for security and defence purposes.	The protection of the human life and Earth environment against natural threats and risks coming from space.

Table 1: Complementary dimensions of Space Security.[86]

Notwithstanding the three dimensions of Space Security are strongly interconnected and interdependent. In order to provide a comprehensive picture of all stakes at play, some aspects related to 'Outer Space for Security' and 'Security from Outer Space' are mentioned throughout the report. For example, users of space systems for ground security and defence operations have strong requirements in terms of service resilience, which reinforce the need to protect space assets from threats.

In this case, it is 'Outer Space for Security' which nurtures the need for 'Security in Outer Space'. Some aspects of these two complementary topics are therefore addressed in this report but special effort was paid to preserve the scope of the study.

[86] Mayence J-F. (2010). 'Space security: transatlantic approach to space governance', *Prospects for transparency and confidence-building measures in space*., (ESPI, Vienna, p 35).

3.1.2 Space infrastructure

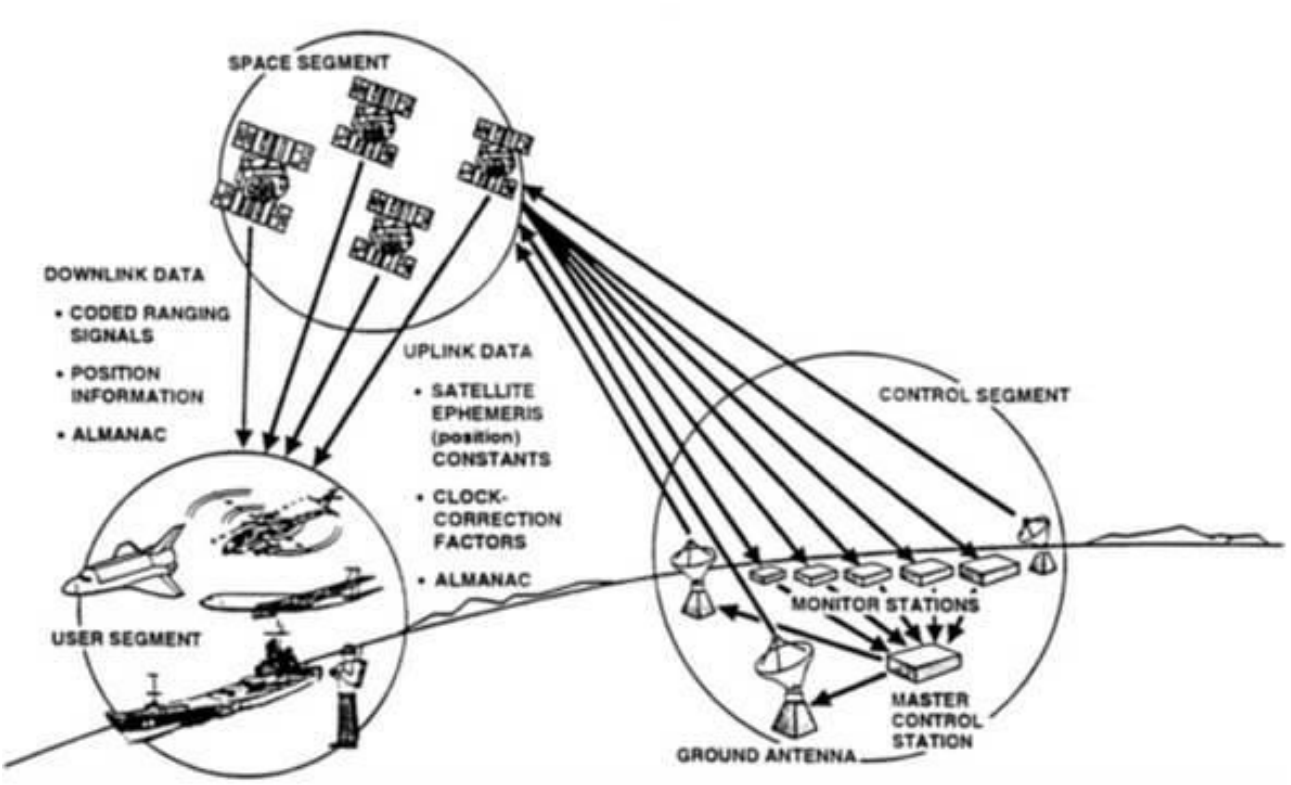

Figure 1: Representation of the GNSS infrastructure components.[87]

As the space infrastructure is the sum of various components, security challenges affecting this infrastructure are also the sum of the different security challenges affecting each component of the infrastructure. The security challenges and threats introduced below are meant to provide an outlook of the different challenges addressed by the study.

- **The space segment** is composed of all systems of the infrastructure located in orbit, namely the satellites and, in general, any spacecraft required for the conduct of operations and delivery of intended service.
- **The ground segment** is composed of all systems of the infrastructure located on the surface of the Earth and necessary for the conduct of operations in space and delivery of data and signals. The ground segment includes stations to interface with the space segment, mission control centres to manage operations in space but also networks

[87] National Research Council, (1995). *The Global Positioning System: A shared National Asset.* (Washington, DC: The National Academies Press,1995).

and terminals to connect the different elements of the ground segment between each other and with other ground systems such as internet and mobile networks.

- **The user segment**, sometimes addressed as a subpart of the ground segment, is composed of complementary ground-based systems required for the delivery of full-fledged space services accessible by end-users. This includes service monitoring centres, data processing facilities or user equipment such as terminals or navigation systems.
- **Downlinks and uplinks** are used to interface between the space and the ground segment (i.e. including users' equipment). Based on radio communication, these signals are used to operate the space system and receive its data.[88] The uplink refers to signals transmitted from the ground to space and the downlink refers to signals received on the ground from space.

As the present report focuses on 'Security in Outer Space', the analysis addresses predominantly security challenges to the space segment. The report addresses, whenever relevant, other security challenges affecting other components of the space infrastructure, in particular intentional and unintentional threats to downlinks and uplinks.

The dissertation focuses on deliberate attacks, even though we acknowledge the existence of other threats, such as unintentional disruption and outages caused by human error, environmental causes or technology failure. Thus, the report does not address security challenges specific to the ground segment such as Earth natural hazards or physical attacks to facilities (e.g. sabotage).

3.1.3 European space infrastructure concept

In the frame of this study, the European space infrastructure is understood as the sum of space and ground assets owned and operated by European public and private stakeholders. The ecosystem of owners and operators of space infrastructure, encompassing space and ground components but also access to space facilities and capabilities includes five main actors:

[88] International Telecommunication Union, (2016). *Measuring the Information Society Report 2016*.

- The European Union (EU), as a supranational institutional actor, owns space infrastructures developed and deployed in the frame of the flagship programmes Galileo, EGNOS and Copernicus. Development, operation and exploitation of EU space infrastructures are delegated to partner organisations including the European Space Agency, the European GNSS Agency (GSA), EUMETSAT and other public and private entrusted entities.
- The European Space Agency (ESA), as an intergovernmental organisation, owns and operates a variety of space systems and ground infrastructures funded from annual contributions by member states governments;
- EUMETSAT, as the European operational satellite agency for monitoring weather, climate and the environment, operate a system of meteorological satellites
- The Member States,[89] who conduct both civil and military programmes and whose national institutions (e.g. space agencies, department of defence) own, operate and exploit national space infrastructures;
- The Commercial Operators, such as Eutelsat, SES, Inmarsat or Spot Image who own, operate and exploit private space infrastructures for a commercial purpose.

Together, these European actors own and operate a wide space infrastructure comprised of numerous space systems and the related ground segment.

3.1.4 Risk management concept

The notion of risk is essential to understand the reality of threats posed to the good functioning of the space infrastructure. The following chart introduces a basic risk management model which brings together various security-related concepts and highlights the relationship between them:

[89] Note: Member States include here a broad coverage of European countries active in space and in particular Member States of the European Union and of the European Space Agency.

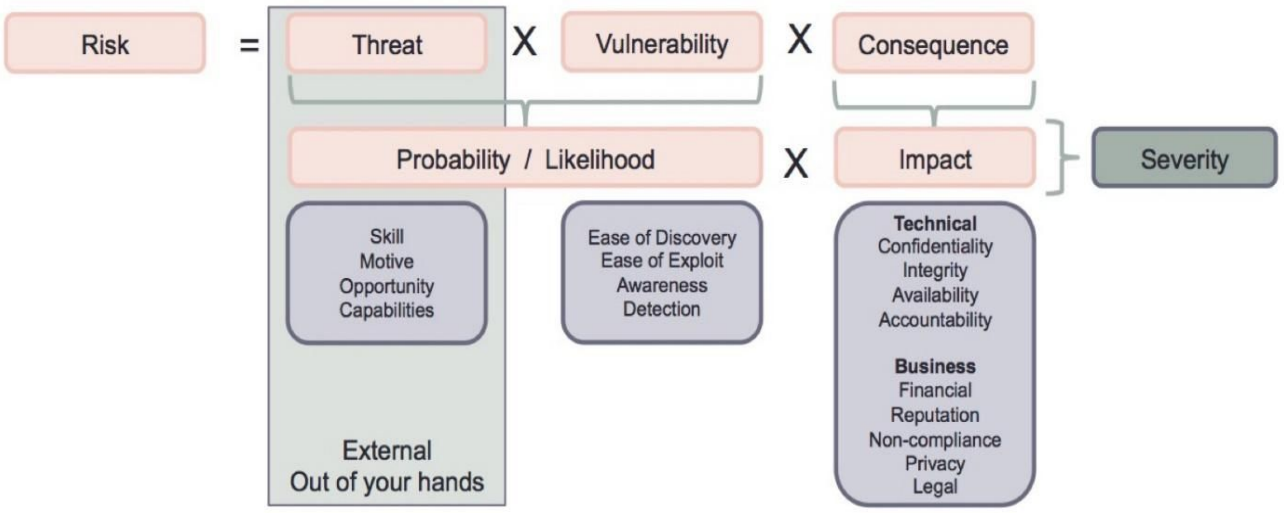

Figure 2: Security-related concepts and relationship between them.[90]

The different concepts included in this model are defined more thoroughly below:

- Threat is defined as 'any circumstance or event with the potential to adversely impact operations or assets'. A threat can lead, purposefully or unintentionally, to the alteration or the destruction of the asset and/or of its operations.
- Vulnerability is defined as 'a weakness in a system, security procedures, internal controls or implementation that could be exploited by a threat source'. A vulnerability is a characteristic of a system that must identified and that can be either eliminated, limited or protected.
- Likelihood is defined, here, as 'a weighted risk factor based on an analysis of the probability that a given threat is capable of exploiting a given vulnerability'. This notion 'combines an estimate of the likelihood that the threat event will be initiated with an estimate of the likelihood of impact'.
- Impact is defined as the magnitude of harm that can be expected to result from the consequences of a threat exploiting a vulnerability.

Risk, as a combination of the above, is therefore defined as the likelihood of a potential loss or damage resulting from the exposition of a system to a threat. This model, initially applied to information systems,[91] shows that risk, which is the essential variable that

[90] Van Impe, K. (2017). 'Simplifying Risk Management'. *Security Intelligence*, (IBM, March 28, 2017).
[91] National Institute of Standards and Technology, (2012). *Guide for Conducting Risk Assessments*, (NIST SP 800-30 Rev. 1, September 2012).

space security activities aim at mitigating, is the product of three specific factors: threat, vulnerability and consequence (or impact). Risk mitigation can therefore be performed through a variety of actions targeted toward threats reduction, vulnerabilities protection or impact mitigation.

3.2 Scope of research

Space technologies, data and services can support numerous EU policies and key political priorities. Therefore, although the European space infrastructure is defined by the conjunction of the European assets (as described section 3.1.3), the study focuses on policies written by the European Union only. The principal reason for this choice is that on a national level, space is often neglected in the wider debate for security. Thus, as a centre for cooperation and global stakeholder to promote space security, the EU as a focus of study is relevant.

3.2.1 The European Union as a space and security actor

Although the space infrastructure has long been used for a variety of security-related applications, recent evolutions in the European foreign, security and defence policy landscape are bringing new challenges and needs to the fore. The institutional setup is also evolving with the European Union taking an increasingly more prominent role in these fields, without undermining the role of Member States. Over recent years, the Union has developed various instruments and policy documents delineating its role, objectives and actions in the field of Security and Defence, and as a result of these developments, security and defence aspects took a noticeable place in the space strategy for Europe endorsed by the Union.[92]

Therefore, the interest and role of the European Union in space security grew within a broader and more political context, as the result of a cross-fertilization between developments of EU mandate in the space domain on one hand and in the security and defence domain on the other hand. In this regard, the Lisbon Treaty (2009) was a

[92] National Institute of Standards and Technology, (2012). *Guide for Conducting Risk Assessments*, (NIST SP 800-30 Rev. 1, September 2012).

stepping stone for both these domains, establishing shared competences between member states and the Union.[93]

As a matter of fact, the EU started considering these domains long before the Lisbon Treaty. At the crossroad, space security progressively gained in importance within European Union priorities. In 2007, the EU and ESA jointly drafted a European Space Policy (ESP), which outlined goals for space programmes, enhanced coordination, and promoted free and independent access to space. The use of European space assets for the fulfilment of security missions, confirmed by the Council of the EU's meeting on 'Taking forward the European Space Policy',[94] led to the conclusion that the "economy and security of Europe and its citizens are increasingly dependent on space based capabilities which must be protected against disruption."[95] It is this underlying principle that fostered a natural expansion of EU perimeter, initially focused on 'Outer Space for Security', to also encompass 'Security in Outer Space'.

Therefore, more recently, the Space Strategy for Europe (2016) highlighted the central place that the EU now give to space security.[96] In the document, references to space security are made transversely across the five EU strategic pillars but are addressed more specifically in the frame of EU objective to 'reinforce Europe's autonomy in accessing and using space in a secure and safe environment'. It is undisputed that today Europe has acquired the status of a full-fledged space power, and that "Space matters for Europe".[97] With a diversity of space programmes for scientific and operational purposes and an autonomous launching capability resulting from a substantial and continuous investment, Europe has joined with full-rights the small club of space powers. As a result, the European Union is equipped today with its own space infrastructure and has developed three flagship programmes: Copernicus, Galileo and EGNOS.

---

[93] European Parliament, (2009). *Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community* (OJ C 306, 17.12.2007); (entry into force on 1 December 2009).
[94] European Parliament, (2008). *Space and security*, (2008/2030(INI)).
[95] European Parliament, (2007). *Taking forward the European Space Policy*, (COM(2007) 212).
[96] European Commission, (2016). *Space Strategy for Europe.* COM(2016) 705 final, (Brussels, 26 October 2016).
[97] *Ibid.*

3.2.2 The United States and the transatlantic partnership to strengthen security

Since its inception, the United States (U.S) space policy compels military, economic and societal considerations. Given the emphasis put on space leadership, security in Outer Space has always been a key driver in both military and civil space activities. Thus, security in Outer Space has long been a strategic interest of the U.S., compelled by military stakes of the Cold War space race as a component of 'space warfare' doctrines. Today, the U.S. space system is the most advanced in the world and relies on a wide national infrastructure[98] operated by military and civilian entities.

Therefore, the singularity of transatlantic relations lies in its extraordinary steadiness through the decades. Since the United States have historic ties to Europe, transatlantic cooperation comes across as a logical follow-up of a long shared history. Space cooperation with European stakeholders was initiated very early in the space age and most of European space programmes benefited from U.S. technical support at the time.

However, the formalisation of such links with the European Union occurred rather recently, with significant effort to achieve that goal started in the 1990s.[99] More recently, the significance of transatlantic dialogue in security matters was widely acknowledged by the 2016 EU's Global Strategy[100] stating that 'a more credible European defence is essential also for the sake of a healthy transatlantic partnership with the United States.' Thus the transatlantic partnership in security is strong and indispensable to ensure a safe cyberspace.[101]

Therefore, the dissertation is focusing on protecting European space infrastructure from cyber-attacks, which would be based on a policy framework crafted by the U.S. National Institute of Standards and Technology (NIST). However, the document is focused on U.S. infrastructure, with no specific accent yet put on space systems. Thus, to efficiently tackle the cyber challenges, the study argue that transatlantic coordination and cooperation will be essential to develop a comprehensive cybersecurity framework for space systems. The wider goal of the thesis is to raise awareness on the topic of

[98] International Astronomical Association, (2017). *Space Traffic Management: Towards a Roadmap for implementation*, IAA Cosmic Study (2017:80).
[99] European Union External Action, (1990). *Transatlantic Agenda*.
[100] European Commission, (2016). *Space Strategy for Europe.* (COM(2016) 705 final).
[101] European Parliament & US House of Representatives, (2017). 'Joint Statement', *81st Inter-Parliamentary Meeting Transatlantic Legislators' Dialogue*, (Washington Dc, 5 December 2017).

cybersecurity for space assets and research further the topic of transatlantic cooperation for space security.

Thus, the research will investigate the treatment of space security challenges in the United States and in Europe. In the United States the research will primarily address the legal, programmatic and technical efforts of governmental bodies involved in space security but will also look into the related and growing activities of commercial stakeholders. In Europe the research will focus primarily on the European Union efforts in the field of space security but will not overlook activities undertaken by European public and commercial partners including the European Space Agency, the Member States and satellite operators. For these different actors, objectives and means will be discussed as components of an overall European approach. Coordination and collaboration between these different actors will also be discussed.

3.3 Research Strategy

The research will primarily address European and U.S. approaches to space cybersecurity and on key areas for transatlantic cooperation development. Document analysis is a social research method and is an important research tool in its own right, and is an invaluable part of most schemes of triangulation, the combination of methodologies in the study of the same phenomenon.[102]

The 2011 U.S. National Security Space Strategy calls for a "multi-layered approach to prevent and deter aggression" against space systems.[103] The security objectives laid out in that strategy suggest a framework of three interrelated means of defending U.S. space assets and guaranteeing the national security communication, observation, and positioning services that those assets provide.

3.3.1 Rationale and data collection

The study choose to use Policy Analysis, and will compare the political provision provided by the European Union to one available in the United States (U.S.). Policy

[102] Bowen, G. A. (2009). 'Document analysis as a qualitative research method'. *Qualitative Research Journal*, 9(2), 27-40.
[103] Department of Defence and ODNI, (2011), *National Security Space Strategy 2011*.

Analysis is a multi-method and multi-disciplinary inquiry designed to create, critically assess and communicate information that is useful in understanding and improving policies.[104] This method is used for problem assessment and monitoring, and therefore provides information on: a) the likely consequences of proposed policies, b) the actual consequences of the policies already adopted. As well, a process through which one identifies and evaluates "alternative policies or programs, are intended to lessen or resolve social, economic, or physical problems."[105]

Policy analysis is a multi-method and multi-disciplinary inquiry designed to create, critically assess and communicate information that is useful in understanding and improving policies. Used for problem assessment and monitoring, and therefore provides information on: a) the likely consequences of proposed policies, b) the actual consequences of the policies already adopted. In order to comprehensively address the security issue, we need to discuss three elements:

Figure 3: Elements of defending space assets.[106]

The first element, system protection measures, includes activities that serve the security objectives to prevent and deter aggression and defeat attacks and operate in a degraded environment. These are primarily technological solutions to enhance the survivability of space systems. The second element comprises deterrence messaging

[104] MacRae, D. & Wilde, J. (1979). *Policy analysis for public decisions*. (Duxbury Press, 1979).
[105] Patton, C. *et al.* (2013). *Basic Methods of Policy Analysis and Planning*. (Taylor and Francis: 2013, 3rd Edition).
[106] U.S. Department of Defense and the Office of the Director of National Intelligence, (2011). *National Security Space Strategy.* (Washington, D.C., January 2011).

measures. The final element of the space defence triad is establishment of coalitions, and international space regimes and norms of behaviour that impose costs to an adversary—in terms of either having to face a coalition or in loss of diplomatic prestige or other sanctions, to prohibit activities taken against another actor's space systems. Each of these three elements has its own attributes and limitations and no single leg is sufficient for defence; thus a combination of them is required to ensure a robust cybersecurity of space assets.[107]

Therefore, in the frame of this Triad for an effective defence for space assets, the study will be looking at the European policy set available to address cyber threats. Thus, to address the first element, we will 1) analyse the European NIS directive;[108] then to address the second element, we will 2) discuss the European Cyber Diplomacy Toolbox; [109] and finally the study will 3) examine the perspective for cooperation on the issue of cybersecurity between the U.S. and Europe through a corpus of literature.

Document	Other name	Redacted by	Origine	Latest update
Framework for Improving Critical Infrastructure Cybersecurity Version 1.1	NIST Cybersecurity Framework	National Institute of Standards and Technology (NIST)	U.S.	April 16, 2018
Directive on security of Network and Information Systems	NIS Directive	European Parliament and Council	E.U.	4 May 2018
Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response	Cyber Diplomacy Toolbox	Council of the Union	E.U.	7 June 2017

[107] U.S. Department of Defense and the Office of the Director of National Intelligence, (2011). *National Security Space Strategy.* (Washington, D.C., January 2011).
[108] European Parliament, (2016). *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*. (Brussels, July 2016).
[109] Council of the European Union, (2017). *Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox")*. (Brussels, 7 June 2017).

to Malicious Cyber Activities				

Table 2: List of chosen policies analysed for the study.

3.3.2 Framework for data analysis

To conduct the analysis, many steps can be followed depending on the policy chosen and the goal to attain.[110] This dissertation processed the policies following the model laid out by Carl Patton,[111] which is as follow:

1. Step One: To define the problem — i.e. verify, define and detail the problem - In order to determine the magnitude and extent of the problem, the study needs to gather information about the problem's antecedent, which will provide knowledge of the issue;
2. Step Two: To establish evaluation criteria — i.e if policy analysis follows these basic steps, which are sequential and causally linked, it involve a much more complex process. The most absorbing aspect of this approach is criteria selection;
3. Step Three: To identify alternative policies — i.e to select a preferred policy, it is necessary to have information about expected outcomes. Thus, thus previous step should give insight to desirable policy outcome, and provide an alternative. The choice for the alternate policy is detailed in section below (3.3.3);
4. Step Four: To evaluate alternative policies — i.e. the analysis of the policies will reveal which alternatives satisfies most of the major criteria, or may call for further examining, or may need for collecting additional data;
5. Step Five : To display and distinguish among alternative policies — i.e present findings;
6. Step Six (if applicable): To monitor the implemented policies — i.e determine success of policy and generated impacts.

[110] Bardach, E. Et al. (2016). *A Practical Guide for Policy Analysis: The Eightfold Path to More Effective Problem Solving. (*Sage Publication*:* 2016*,* Fifth Edition).
[111] Patton, C. *et al.* (2013). *Basic Methods of Policy Analysis and Planning*. (Taylor and Francis: 2013, 3rd Edition).

Policy analysis may take various routes through analysis because of the differences in complexity of the problem, resources, time restraint, and organisation. Considering that the U.S. NIST and the EU NIS are not entered into force, the study will focus on the point a), and can thus disregard step six of analysis.[112]

3.3.3 Choice of alternate policy

The European Union (EU) and the United States are the leading hubs of global information and communications networks that strengthen the deep economic, political, and social ties between these two unions and link each of them with the rest of the world. These networks face cyber threats that are global in origin, indifferent to national borders, and common to both sides of the Atlantic. It is the use of reason and evidence to select the best policy among number of alternatives to address a particular policy issue, as well as a process through which one identifies and evaluates "alternative policies or programs that are intended to lessen or resolve social, economic, or physical problems."[113]

The Step Three of the analysis requires to choose an alternate policy. The Step Three of the analysis requires to choose an alternate policy. The proposal submitted back in September mentioned the alternate policies would be the NIST Cybersecurity framework and the ISO 27000 family of standards, with specific reference to ISO/IEC 27001 and 27002. After more study on the topic, the latter was not considered relevant as it is not a risk-based document, contrary to what is recommended by the literature:

> "The requirement is rather to *manage* rather than try to *eliminate* threats and risks that reside in cyberspace, or those that use cyberspace as an attack pathway. Furthermore, rather than hoping to be able to prevent every imaginable cybersecurity threat and attack, a more practical approach must be to create a cybersecurity regime that is centred on security-by-design and *pre-emptive* risk mitigation controls with the flexibility and resilience to handle emergencies as they develop".[114]

[112] Weimer, D. *et al.* (2017). *Policy Analysis: Concepts and Practice*. (Routledge: 2017).
[113] *Ibid.*
[114] Livingstone, D. & Lewis, P. (2016). "Space, the Final Frontier for Cybersecurity? ", *Chatham House Research Paper*, p.24.

The study however, kept the NIST Cybersecurity Framework as relevant alternative to the European policy. The rationale behind choosing this U.S. policy has several aspects:

- The existing similarities between the European Union and the United States;
- The two groups are the most important space players in the World;
- The EU and the U.S. are 'like-minded countries';
- The two groups are subjected to the same cyber risks to their infrastructure.

	European Union	**United States**	**Source**
Population	508,943,606 (2017)	324,459,463 (2017)	United Nations (2017). *World Population Prospects - Population Division - United Nations*. Retrieved 9 March 2018.
GDP (PPP)	$20.853 trillion (2017)	$19.417 trillion (2017)	International Monetary Fund (2017). *Report for Selected Countries and Subjects*. Retrieved 9 March 2018.
Area	4,324,782 km^2 (1,669,808 sq mi)	9,826,630 km^2 (3,794,080 sq mi)	Central Intelligence Agency (2015). 'Field Listing – Area'. *The World Factbook*. Retrieved 9 March 2018.
Defence spending	€206 billion (2016)	€546 billion (2016)	World Economic Forum (2017). 'IISS Military Balance 2012/2017'. *Does Europe contribute*

			enough to NATO. Retrieved 9 March 2018.
Space spending	€12,305 million (EU + Member States, 2016)	€35,957 million (2016)	Euroconsult (2017). *Government Space Programs: Benchmarks, Profiles & Forecast to 2026.* Retrieved 9 March 2018.
Cybersecurity risk to their space infrastructure	High (2017)	High (2017)	Harrison, T. *et al.* (2018). *Space Threat Assessment 2018. Aerospace Security, CSIS (April 11, 2018).*

Table 3: Ground for comparison between the EU and the U.S.

Moreover, the United States and the EU cooperate on cybersecurity and cyber-defence in a variety of forums. Under a NATO Technical Arrangement, the United States and EU exchange threat information, share best practices, and cooperate with industry partners.The United States and all EU member states are signatories to the Council of Europe Convention on Cybercrime (or Budapest Convention) and collaborate on cybersecurity in multilateral organisations, including the United Nations Group of Experts, the Organisation for Security Cooperation in Europe, Organisation for Economic Cooperation and Development, Interpol, the G7 and G20 country groups, and others. Since 2010, a joint EU-U.S. Working Group on Security and Cybercrime has conducted annual exchanges, public-private workshops, and tabletop exercises.[115]

[115] European Union – External Action (2014). *Fact Sheet: EU-US cooperation on cyber security and cyberspace*, (26 March 2014).

3.4 Limitations

This study will attempt to investigate the usefulness of a space-cyber framework for better governance. However, because the study will be conducted from a transatlantic perspective, it cannot answer for the entire space community, which is composed of various actors from multiple industries and countries around the globe, and who all have different interests and values in the crafting of space governance.

Unfortunately, due to time constraint, the study will not incorporate interviews, which would have been conducted end of May in the United States.

Finally, the study acknowledges cultural biases might affect the direction and result of this study, as the dissertation will be conducted from a European point of view.

IV. Findings

This chapter presents the key findings that were made during this study. These findings are provided by the analysis of the cybersecurity policies. In order to effectively build a cybersecurity for Outer Space, it is first important to understand the nature of the threat as well as to evaluate the risk.

Therefore, the study first provide knowledge of the problem and determine the magnitude and extent of the issue. Secondly, the study provides an easy understanding of the nature of space cyber threats before presenting the major security risks stemming from a state-sponsored attack. Then, the study evaluates the European policies in addressing the cyber threat. Finally, the dissertation will offer a reflexion on the alternative policy and the development of governance through a strengthening of the transatlantic partnership.

4.1 Providing a common understanding of the nature of the risk

Comparably to other infrastructures relying on cyber to operate, the space infrastructure can be the target of cyberattacks which include a range of offensive manoeuvres against computer and information systems to steal, disrupt or destroy a specified target (e.g. data, service, system) by hacking into the network. However, until the Tallinn Manual of 2013,[116] governments and organisations did not agree on what represented a cyber attack.

4.1.1 The different nature of the cyber threats

The strategic value of space to the EU has been recognised in numerous areas that benefit European citizens, including earth observation, location-based services, navigation, and also security and defence aspects.[117] Much of the world's critical infrastructure – such as communications, air transport, maritime trade, financial and other business services, weather and environmental monitoring and defence systems –

[116] CCDCOE (2013). *NATO's Tallinn Manual*, (Cambridge University Press).
[117] Pindják, P. (2016). "A Stronger EU in Cosmos: Embracing the Concept of Space Security", *INCAS BULLETIN*, (Volume 8, Issue 3).

depends on the space infrastructure, including satellites, ground stations and data links at national, regional and international levels.[118] From a practical perspective, cyber-attacks targeting the space infrastructure include a variety of possible manoeuvres pursuing in general the objective to 1) steal information (e.g. data, communications) and/or 2) disrupt the space infrastructure (e.g. systems, operations, capabilities, services). Threats also include cyberattacks that do not target directly the space infrastructure but rather exploit its vulnerabilities as a mean to reach other infrastructures and systems.

Therefore, threats are categorised according to the five types of threat identified in the NIST definition, these threat types can be connected to the core principles of the concept of information security: confidentiality, integrity and availability.[119] Threats can be categorised as follow: destruction of data; modification of information; unauthorised access; disclosure of data; and denial of service. Thus, cyber attacks can be grouped in the following categories, with the most sophisticated attacks resulting from a combination of different types of attacks:[120]

- System Compromise to obtain temporarily the control of a system and consequently the capacity to execute arbitrary commands or to gain a foothold in the network to carry out other attacks;
- Service Disruption to prevent a system from performing as expected with consequences ranging from reduced quality of service to total system failure;
- Data Exfiltration to steal sensitive information from a target for reconnaissance, strategic intelligence, theft or to expose secret information;
- Bad Data Injection to submit incorrect data (e.g. erroneous TT&C data) to a system without detection with a range of possible consequences;
- Advanced Persistent Threat (APT) to gain extended access to a system and get permanent and undetected capacity to access system information or take control of the system.

[118] Livingstone, D. & Lewis, P. (2016). 'Space, the Final Frontier for Cybersecurity?', *Chatham House Research Paper*.
[119] National Institute of Standards and Technology, (2004). *Standards for Security Categorization of Federal Information and Information Systems*. (FIPS PUB 199).
[120] Lu, M. (2014). 'Types of Cyber Attacks', *TCIPG*, (September 12, 2014).

Moreover, the report by the Chatham House also underlines the following potential methods:[121]

- Attacks on satellites, by targeting their control systems or mission packages, perhaps taking control of the satellite to exploit its inherent capabilities, shut it down, alter its orbit (perhaps thereby 'weaponizing' it), or 'cook' or 'grill' its solar cells through deliberate exposure to damaging levels of highly ionising radiation;
- Attacks on the ground infrastructure, such as satellite control centres, the associated networks and data centres, leading to potential global impacts (for example on weather forecasting systems, which use large quantities of space-derived data).
- Hacking attacks on, for example, communication networks, by using space infrastructure.

Therefore, among malicious interferences include all intentional disruptions or deceptions of uplink or downlink signals aiming to disturb space systems operations and/or delivery of space-based services.[122]

4.1.2 The singularity of jamming and spoofing data links

Malicious interferences include two main categories of threats: jamming and spoofing. Jamming is a type of signal-based attack that aims to disrupt authorised radio communication signals. From a technical perspective, malicious interferences usually involve the emission of rogue radio signals that disrupt a target signal by decreasing its signal-to-noise ratio.[123] Jamming can be done at any point of the communication channel: at both ends, in space and on the ground by directly targeting satellites, ground stations or user equipment communication subsystems (i.e. antennas, receivers, emitters, transponders…) and by interfering locally with radio signals at any point between space and ground systems.[124]

---

[121] Lu, M. (2014). 'Types of Cyber Attacks', *TCIPG*, (September 12, 2014).
[122] Eutelsat, (2013). 'Satellite Interference: an Operator's Perspective', *ITU*: [https://www.itu.int/en/ITU-R/space/workshops/2013-interference-geneva/presentations/Ethan%20Lavan%20-%20Eutelsat.pdf], (June 10, 2013). (Accessed 23 January, 2018).
[123] International Telecommunication Union, (2017). 'About GCA', *Global Cybersecurity Agenda* (GCA), [https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx]. (Accessed November 12, 2017).
[124] Consultative Committee for Space Data Systems, (2015). 'Security Threats Against Space Missions', *Report Concerning Space Data System Standards*, (CCDS 350 1-G-2, December, 2015).

Therefore, numerous examples of satellite jamming occurred in the recent years. For example, in 2010, the UN leading communication agency called on Iran to end jamming of satellite broadcasts,[125] during the Arab Spring in 2010-2012 satellite jamming rose dramatically in quantity and duration targeting news agencies notably BBC Middle East, France 24, Deutsche Welle and the Voice of America.[126]

Moreover, spoofing is a type of signal-based attack (i.e. software-based spoofing is addressed later as a type of cyberattack) that aims to deceive a receiver by broadcasting incorrect signals structured to resemble genuine signals or by rebroadcasting genuine signals captured at a different location or time.[127] Spoofed signals target the receiver part of the communication channel which can include satellites in the case of spoofed uplink signals or, more commonly, ground stations and user equipment in the case of spoofed downlink signals.[128] One of the most noticeable example of spoofing took place in the Black Sea when the U.S. Maritime Administration reported 20 affected ships near the coast of Novorossiysk.[129]

Therefore, these threats can seriously affect the quality of space-based services and therefore lead to substantial impacts on operations dependent on these services such as road, rail, air and water transport or civil protection among many others.[130] Here again, the threat is ubiquitous and inclusive. From a legal standpoint, both jamming and spoofing are a violation of the International Telecommunication Union Convention.[131] However, loopholes in enforcement mechanisms make it difficult to either prevent or

[125] Nebehay, S. (2010). 'U.N. tells Iran to end Eutelsat satellite jamming', *Reuters*: [https://www.reuters.com/article/us-iran-jamming-itu/u-n-tells-iran-to-end-eutelsat-satellite-jamming-idUSTRE62P21G20100326], (March 26, 2010). (Accessed 23 January, 2018).
[126] Director General's Office, (2012). 'EBU Deplores Middle East Satellite Jamming', EBU: [https://www.ebu.ch/contents/news/2012/10/ebu- deplores-middle-east-satelli.html], (October 22, 2012). (Accessed 12 November, 2017).
[127] International Telecommunication Union, (2017). 'About GCA', *Global Cybersecurity Agenda* (GCA), [https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx]. (Accessed November 12, 2017).
[128] Consultative Committee for Space Data Systems, (2015). 'Security Threats Against Space Missions', *Report Concerning Space Data System Standards*, (CCDS 350 1-G-2, December, 2015).
[129] Hambling, D. (2017). 'Ships fooled in GPS spoofing attack suggest Russian cyberweapon', *New Scientist*, [https://www.newscientist.com/article/2143499-ships-fooled-in-gps-spoofing-attack-suggest-russian-cyberweapon/], (2017, August 10). (Accessed February 5, 2018).
[130] Consultative Committee for Space Data Systems, (2015). 'Security Threats Against Space Missions', *Report Concerning Space Data System Standards*, (CCDS 350 1-G-2, December, 2015).
[131] International Telecommunication Union, (2017). 'About GCA', *Global Cybersecurity Agenda* (GCA), [https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx]. (Accessed November 12, 2017).

punish it.[132] Production, commerce and / or use of jamming and spoofing devices are illegal in various countries.[133] Despite being illegal, reports suggest that these devices are becoming increasingly simple to procure and use.

Moreover, traditional vectors of attack, such as jamming a signal — seen as a major threat just a few years ago — are quickly being replaced by more complex threats. These include sophisticated spoofing attacks or Advanced Persistent Threat (APT), i.e. establish and extend its presence within the information technology infrastructure (e.g. a satellite) for purposes of exfiltrating information, undermining or impede critical aspect of an organisation or government; or positioning itself to carry out these objectives in the future.[134] The table visualises the various capability levels of various threat agent groups: threat agents who are the source of many primary threat actions are the ones with higher capabilities, while with ones with more secondary or no cyber-threat assignment are possess lower capabilities.

			Actors		
Nature of threats		Effects	Cyber-criminals	Hacktivists	Nation-states
Service disruption	**Jamming**	- prevent the system from performing as expected; - reduced quality of service; - temporary stopping of signal.	NO	YES	YES
	Spoofing	- prevent the system from performing as expected; - system failure; - exchange of wrongful signal.	NO	YES	YES
System compromise	**Data breach**	- stealing of sensitive information for reconnaissance, strategic intelligence, theft;	YES	YES	YES

[132] Jakhu, S. (2013). 'Satellites: Unintentional and Intentional Interference', *Secure World Foundation*. (June 17, 2013).
[133] Federal Communications Commission, (2018). 'Jammer Enforcement', *FCC*, [https://www.fcc.gov/general/jammer-enforcement]. (Accessed May 12, 2018).
[134] National Institute of Security and Technology,(2018). 'Advanced Persistent Threat'. *NIST SP 800-39*, [csrc.nist.gov/Glossary/?term=2856]. (Accessed on May 5th, 2018).

		- capacity to expose secret information.			
	Advanced Persistent Threat (APT)	- gain extended access to a system; - permanent and undetected capacity to access system information; - take control of the system.	NO	NO	YES

Table 4: Simplified matrix of cyber threat to on-orbit space infrastructure.

4.2 Nation-States as the threat actors

Malicious interferences are also a growing component of warfare with opponents seeking to deny or exploit satellite support to ground operations (e.g. positioning and navigation, telecommunication).

The cyber threats are sure to grow as space serves as a force-multiplier for global power projection, and influence on how these risks and threats impact on broader security architectures.

4.2.1 Motivations behind state-sponsored attacks

Motivations behind such obstruction or misinformation attempts are multiple, ranging from government censorship to deny a population with access to satellite-based information services to logistics professionals seeking to block or deceive the monitoring of their position. The first known space asset targeted by a cyber-attack was the German ROSAT satellite in 1998.[135] A senior advisor at the American National Aeronautics and Space Administration (NASA) reported in a classified document that the failure was due to "cyber-intrusion" operated by the Russian government into NASA's network.[136] However, the official investigation released publicly in 2008, claimed the ROSAT incident was

[135] Pasco, X. (2015). 'Various Threats of Space Systems', *Handbook of Space Security*, (Kai-Uwe Schrogl & al., eds., Springer, 2015, p. 673–674).
[136] Talleur, T. (1999). *Russian Domain Attacks Against NASA Network Systems*. Not publicly published. Classified as "For Official Use Only - No Foreign Dissemination". Inspector General's Office, NASA.

simply "coincident with intrusion".[137] Since, cyber-attacks targeting the assets in operation continued to be reported at quicker intervals, raising international security concerns.[138]

Therefore, in 2002, a SinoSat satellite was hacked to broadcast contents promoting the cult of Falun Gong, forbidden in China, on national television for four hours.[139] In 2007, the Sri Lankan terrorist group Tamil Tigers managed to broadcast on TV and radio in Europe and Asia through Intelsat satellite transponders.[140] Landsat 7 and Terra (EOS AM-1), two American satellites operated by NASA, were respectively hacked in 2007 and 2008.[141] These two attacks were linked to the Chinese government, although no formal evidence has been brought forward. Following the incident NASA ran an audit in 2001, and reported that six computer servers controlling spacecraft contained vulnerabilities that could be exploited by remote attackers.[142] However, and despite the alarming report, the cyber threat remained largely unrecognised as a potentially significant vulnerability for space assets, and stayed unaddressed in practical mechanisms.[143]

Therefore, it is proven and seen that nation-states can use cyberattacks against space assets in two ways: cyber-espionage, and cyber-warfare disruptions.[144] Until recently, cyber-espionage on space assets was largely confined to the economic domain, with states sponsoring in some cases. The main risk, from a business perspective, pertain to intellectual property infringements, disclosure of trade secrets, and economic espionage. However, the crossroad between cyber and space is now also increasingly being used for political purposes.

---

[137] Elgin, B. (2008). "Network Security Breaches Plague NASA", *Bloomberg*, (20 November 2008).
[138] UK HM Government (2014). *National Space Security Policy*, (UKSA/13/1292, p. 2).
[139] Hogg, C. (2004). 'HK probes Falun Gong 'hacking'. *BBC News*, [http://news.bbc.co.uk/2/hi/asia-pacific/4034209.stm], November 23, 2004. Accessed 23, January 2018.
[140] McCoy, J. (2007). *Intelsat Shuts Down Transponder Hijacked By Terrorists*. *Via Satellite*: [http://www.satellitetoday.com/uncategorized/2007/04/26/intelsat-shuts-down-transponder-hijacked-by-terrorists/]. (April 26, 2007). (Accessed November 13, 2017).
[141] U.S. Government Printing Office (2011). *2011 Report to Congress of the U.S.-China Economic and Security Review Commission*, (pp. 215–217). (Accessed on Dec 12, 2017).
[142] Pasco, X. (2015). 'Various Threats of Space Systems', *Handbook of Space Security*, (Kai-Uwe Schrogl & al., eds., Springer, p. 673).
[143] Livingstone, D. & Lewis, P. (2016). 'Space, the Final Frontier for Cybersecurity?', *Chatham House Research Paper*.
[144] Grisham, P. (2017). "Satellite Cybersecurity and Information Assurance: How Secure Are Our Nation's Satellites?". *Keynotes from CompTIA webinar,* (March 1, 2017).

Therefore, cyber-attacks are emerging as a new instrument for both state and non-state actors to pursue specific geostrategic interests. In fact, for many countries, as for non-state actors, cyber tools offer an attractive weapon: cheap, effective, high-impact, difficult to trace.[145] China and Russia are regularly pointed out as the main countries actively sponsoring cyber-attacks, with the World's most effective hackers said to be located in Russia.[146] A famous example of cyber-espionage using space assets was done by the Russian-led Turla group, which hacked into satellites to gain access to sensitive and confidential information of western embassies, government institutions, and military entities between 2008 and 2016.[147] The attack was used against forty-two countries, among which figured the United States (U.S.) and six European States (France, Germany, Latvia, Poland, Serbia, Spain).[148] Moreover, Russia, used jamming and spoofing attacks in 2015 against the American Global Positioning System (GPS) in order to cover their progression in Crimea.[149]

Therefore, Nation states may aim to target other states for geopolitical reasons.[150] Moreover, Nation States being threat actors in the space domain raise the issue of the increasing connection between activities in space and geopolitical tensions on Earth.[151] Indeed, both cyber and space is considered key warfighting domains, and their importance for national security makes them a vital target in a military altercation.[152]

---

[145] Lipton, E., et al. (2016). 'The Perfect Weapon: How Russian Cyberpower Invaded the U.S.', *The New York Times*, (13 December 2017).

[146] Bennett, C. (2015). 'Kremlin's ties to Russian cyber gangs sow US concerns', *The Hill*, (10 November 2015).

[147] Nakashima, E. (2015). 'Russian hacker group exploits satellites to steal data, hide tracks', *The Washington Post*, (September 9, 2015).
[148] Tanase, S. (2015). 'Satellite Turla: APT Command and Control in the Sky', *Kaspersky Lab*, (Sept. 9, 2015).
[149] Pomerleau, M. (2016). 'Threat from Russian UAV Jamming Real, Officials Say', *C4ISRNET,* (Dec 20, 2016).
[150] National Counterintelligence and Security Center (2014). *National Counterintelligence Strategy of the United States*.
[151] Robinson, J. (2017). Deterring Chinese and Russian space hybrid warfare by economic and financial means, *The Space Review*, (September 18, 2017).
[152] Asbeck, F. (2014). "An EU View: Comparisons and Establishing Norms in the Cyber and Space Domains", in *Chatham House*, (December 2014, p.42).

4.2.2 Geopolitical Consequences of state-sponsored cyber attacks

Hostile acts or acts that are perceived as being hostile in either domain could jeopardise international relations and stability and even lead to conflict.[153] States such as North Korea and Iran, are officially investing their scarce resources in such space technologies in the name of "peaceful uses of space".[154] Hence, as more countries integrate space into their national military capabilities and rely on space-based information for national security, there is an increased chance that any interference with satellites could spark or escalate tensions and conflict in space or on Earth.[155] Indeed, both cyber and space is considered key warfighting domains, and their importance for national security makes them a vital target in a military altercation.[156]Indeed, Russia already stated that the information domain, provided by satellites systems, is one of war, [157] and the United States mentioned that a purposeful disruption of space capabilities by a cyber-attack could be considered an act of war.[158] Thus, purposeful interference with space systems could rather easily trigger a retaliatory spiral of actions.[159]

Although Russia denies to interfere in foreign affairs, there is increasing evidence of the involvement of Russian hackers in many strategic attacks. In Russia's case, cyber warfare through space appears to be becoming a fully-fledged component of an aggressive foreign policy — combining the fourth and fifth domains after land, sea and air.[160] Though so far below the threshold of outright war, cyber aggression on space assets is emerging as a major disruptive element that can be activated to achieve strategic superiority and destabilise States.[161] A disruption or shutdown of space systems

---

[153] Asbeck, F. (2014). "An EU View: Comparisons and Establishing Norms in the Cyber and Space Domains", in *Chatham House*, (December 2014, p.42).
[154] Suzuki, K. (2016). "How Governance Models Affect Geopolitics: The Asian Case Study", *Yearbook on Space Policy 2014*. (C. Al-Ekabi et al. (eds.), Springer-Verlag Wien, p.199).
[155] Robinson, J. (2017). Deterring Chinese and Russian space hybrid warfare by economic and financial means, *The Space Review*, (September 18, 2017).
[156] Asbeck, F. (2014). 'An EU View: Comparisons and Establishing Norms in the Cyber and Space Domains', *Chatham House working paper*, (December 2014, p.42).
[157] Geers, K. (2015), *Cyber War in Perspective: Russian Aggression against Ukraine*, (Tallinn: NATO CCD COE, p. 20).
[158] Clark, C. (2016). "Cyber Attack On Satellite Could Be Act Of War: HPSCI Ranking", *Breaking Defense,* (May 4, 2017).
[159] Robinson, J. (2016). "Governance challenges at the intersection of space and cyber security". *The Space Review*, (February 15, 2016).
[160] Foxall, A., '*Putin's Cyberwar: Russia's Statecraft in the Fifth Domain*', Russia Studies Centre, Policy Paper No. 9, May 2016.

[161] European Commission (2017). 'Building an Effective European Cyber Shield: Taking EU Cooperation to the Next Level'. *EPSC Strategic Notes*, (Issue 24, 8 May 2017).

would cause disastrous knock-on effects on other key infrastructures and sectors, leading to possible waves of economic crises,[162] as well as putting human life at risk of harm or loss.[163] The cyberthreat used in greater intensity and accuracy toward space systems, moving ever closer to the sphere of space and cyber wars that would fall within the remit of Article 5 of the NATO Washington Treaty.[164]

Therefore, the use of cyber-attacks on space systems are likely to undermine political and strategic stability in the near future.[165] Consequently, acts that are perceived as being hostile in either domain could jeopardise international relations and stability and even lead to conflict.[166] Thus, not only the disruption of capabilities that space assets provide would have immediate, far-reaching and devastating economic and social repercussions, it would also have political and geo-strategic consequences.[167]

Therefore, an attack on a space asset through cyberspace has many advantages over a kinetic attack, not least of which is that it offers plausible deniability in some cases, or can be masked as defensive even if conducted for offensive purposes.[168] Moreover, the anonymity offered by cyber-attacks is appealing to states willing to hack satellites in order to compromise foreign networks, or cover illegal activities.[169] This raise the main issue regarding the cyber threat: the question of attribution. Thus, an important step forward in addressing these challenges by developing space governance in order to increase strategic stability and security.[170]

---

[162] PwC (2018). *Dependence of the European Economy on Space Infrastructures,: Potential impacts of space assets los*s. EU publications, (February 2018).

[163] Grisham, P. (2017). 'Satellite Cybersecurity and Information Assurance: How Secure Are Our Nation's Satellites?', *Keynotes from CompTIA webinar,* (March 1, 2017).

[164] The key section of the Article 5 of the NATO Washington Treaty is the collective defence clause, committing each Member State to consider an armed attack against one Member States, in Europe or North America, to be an armed attack against them all.

[165] Secure World Foundation, (2015). *Strategic Stability and Space*.
[166] Grisham, P. (2017). "Satellite Cybersecurity and Information Assurance: How Secure Are Our Nation's Satellites?", *Keynotes from CompTIA webinar*, (March 1, 2017).
[167] Robinson, J. (2016). "Governance challenges at the intersection of space and cyber security". *The Space Review*, (February 15, 2016).
[168] Robinson, J. (2017). Deterring Chinese and Russian space hybrid warfare by economic and financial means, *The Space Review*, (September 18, 2017).
[169] Tanase, S. (2015). 'Satellite Turla: APT Command and Control in the Sky', *Kaspersky Lab*, (Sept. 9, 2015).
[170] Weeden, B. & Chow, T. (2015). "Developing a framework and potential policies for space sustainability based on sustainable management of common-pool resources", *Secure World Foundation*.

4.3 The European Cybersecurity Policies as a mitigation tool

Cybersecurity is an area of shared competence between the EU as a whole and its individual member states. Although member states have responsibility for security and law enforcement, as well as critical infrastructure such as communications and energy, the EU plays an increasing role. Cybersecurity has emerged as a top EU security priority because of the impact of cyber risks on the EU economy and the single market, as well as the attendant need for cooperation across borders.

4.3.1 The incentive and constraint of information-sharing

The term 'cybersecurity' in Europe has remained vague and encompassed an array of issues ranging from responsibility, freedom and openness, trust, the protection of privacy, the combat of cybercrime.[171] To ensure better cooperation between Member States, the European Parliament voted to adopt the draft NIS Directive as part of an EU cybersecurity effort of harmonisation that targets the creation of uniform standards and levels of cybersecurity across the EU, ie. the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure.[172]

The cyber security industry is rife with examples of limited information sharing.[173] Sharing of information about cyber threats or incidents — whether by providers giving notification to relevant authorities, entities cooperating with each other, or relevant authorities sharing with each other through a cooperation group — has been a growing element of national cybersecurity policies. Data breach notification to public authorities is one form of information sharing. While the NIS Directive contains mandatory breach notification obligations, it also recognises the tensions between the public and private interests in disclosing breaches. The issue is, that there is still no framework for information-sharing in Europe related to the space domain.

---

[171] Csernatoni, R. (2016). 'Time to Catch Up: The EU's Cyber Security Strategy', *European Public Affairs*, (March 4, 2016).
[172] European Union for Foreign Affairs and Security, (2013). *The Cybersecurity Strategy of the European Union – An Open, Safe and Secure Cyberspace*. JointCOM(2013) 1 Final. (Brussel, February 7, 2013).
[173] Bardin, J. (2014). "Satellite Cyber Attack Search", *Cyber Security and IT Infrastructure Protection*, (Elsevier Inc, p.317).

Therefore, methods of remediation that are successful should be shared across the satellite industry and within federal and state governments. The opportunity to share effective security practices could vastly improve satellite cyber defenses. Information sharing coupled with the appropriate education and awareness-raising efforts for the satellite industry is an effective method of propagating actionable intelligence. Most companies are remiss to share information on breaches due to the potential embarrassment public awareness could bring. What is missed is the opportunity to share remediation strategies and information on the attacker. This actionable intelligence could prevent other organisations from suffering the same fate.

Therefore, under the NIS Directive, member states are required to adopt a national cybersecurity strategy that will ensure a high level of security for network and information systems if deemed "essential". It requires member states to operate national cybersecurity governance frameworks and ensure that operators of such services take "appropriate measures" to manage risks to their networks. In particular, in seeking to balance these interests the NIS Directive provides that notification shall not make the notifying party subject to increased liability.

Therefore, the Cybersecurity Directive envisaged creating Computer Emergency Response Teams (CERTs) in each EU Member States as well as fostering cooperation and information exchange obligations between Member States and the Commission. However, the implementation of such standards depends on the Member States' willingness to redirect funds specifically for cyber defence, to share critical information, or their determination to pass targeted legislation on cyber security.

4.3.2 Accountability and Deterrence: The Cyber Diplomatic Toolbox

Deterrence is the process of convincing an opponent that the costs of attack will outweigh the benefits. This can be done by holding at risk things of value to the adversary (threats of retaliation), by convincing him that he will not achieve the goals of his attack (denial of benefit), and by increasing his level of uncertainty – or some combination of these.[174] In space there are unique issues and several obstacles to deterrence strategies. These might be summarised in three categories: 1) The vulnerability gap in space; 2) the

[174] Harrison, R. (2015). 'The Role of Space in Deterrence', *Handbook of Space Security*, (Kai-Uwe Schrogl & al., eds., Springer).

difficulty of defending satellites; and 3) the weakness of space situational awareness/attribution of attack.

Therefore, the clear advantage of a cyber-attack is that unlike a missile, cyber attacks can travel internationally through cyberspace in moments, implicating computers in countries far from the original location of the hacker.[175] The capability to detect the origin of the attack and to attribute its responsibility will be the key for an effective deterrence strategy.[176] However, Currently, no mapping and affective deterrent structures exist addressing space hybrid risks and attacks - ie. via established norms, active dissuasion, or accountability/enforcement measures.[177]

Therefore, without a mechanism to enforce regulation, each individual actor will be tempted to not comply to the set "rules of the road", because defection will leave it better off, especially if other actors do not retaliate.[178] Without mechanisms for identifying and enforcing violations of the rules each actor would have an incentive to cheat but if everyone cheats everyone will be worse off than they would have been if the rules had been adhered to.[179]

Therefore, the Council of the European Union, which represents the heads of state and government of the European Union, developed a "Cyber Diplomatic Toolbox"— a framework for joint EU diplomatic responses to malicious cyber activities.[180] The Council clearly perceives the toolbox as a deterrent. Its statement stresses that is signaling the likely consequences of a joint EU diplomatic response to malicious cyber activities, thus hoping to reinforce the security of the EU and its Member States.[181] The toolbox was published after when diplomatic efforts aimed at regulating states' behavior in cyberspace were struggling, and attacks against information systems were becoming more pervasive.[182]

---

[175] Landler, M. & Markoff, J. (2007). "Digital Fears Emerge After Data Siege in Estonia", *New York Times*, (May 29, 2007).
[176] Pasco, X. (2015). 'Various Threats of Space Systems', *Handbook of Space Security*, (Kai-Uwe Schrogl & al., eds., Springer, p. 673-674).
[177] Jana Robinson (2017). 'Deterring Chinese and Russian space hybrid warfare by economic and financial means', *The Space Review*, (September 18, 2017).
[178] Robinson, J. (2016). "Governance challenges at the intersection of space and cyber security". The Space Review, (February 15, 2016).
[179] Aliberti, M. & Krasner, S. (2016). "Governance in Space", *Yearbook on Space Policy 2014.* (C. Al-Ekabi et al. (eds.), Springer-Verlag Wien, p.145).
[180] Council of the European Union (2017). *Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox")*. (Brussels, 7 June 2017).
[181] *Ibid.*
[182] De Zan, T. (2017). 'Deterring "bad hombres": the EU cyber diplomatic toolbox', *Italian Institute for International Security Policy*, (October 20, 2017).

Therefore, the initiative of the Cyber Diplomatic Toolbox may open a new and important page in European cyber deterrence, but only if it is supported by a strong political commitment, and if the broader context is understood.[183] Next to the common diplomatic tools, such as making statements of condemnation, summoning ambassadors, or declaring diplomats persona-non-grata, this means that there can be serious a consideration of political and economic sanctions against any adversary attacking EU member states in cyberspace.[184] However, the diplomatic response is sometimes not enough, especially if the impacts of cyber attacks are severe.

Therefore, although build to be an incentive in deterring state actors, it is hard to think that rogue state actors would be seriously deterred by the prospect of diplomatic retaliation. It is difficult to imagine how diplomatic responses like sanctions would work in practice without attribution. However the EU notes that a determination of attribution is not required for the toolbox to be used, and in that regard, the EU stresses that not all measures of a joint EU diplomatic response to malicious cyber activities require attribution.[185] Thus, the diplomatic retaliation tools may function as a deterrent, making cyber attack less anonymous and risk-free, while also bringing with them little danger of immediate escalation.

Therefore, measures like diplomatic demarches can be taken without presenting any evidence, to show that certain malicious behavior is being detected and should end. Such diplomatic signaling is a useful instrument to make malicious cyber operations less anonymous and risk-free while bringing little danger of immediate escalation.[186] It is also thinkable that the EU added this attribution formula to express some flexibility which would contribute to the toolbox's deterrent effect.

[183] Limnell, J. et al. (2017). 'EU cyber diplomacy requires more commitment, *EU Observer*, (July 7, 2017).
[184] Council of the European Union (2017). *Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox")*. (Brussels, 7 June 2017).
[185] *Ibid.*
[186] Segal, A. (2017). 'EU Creates a Diplomatic Toolbox to Deter Cyberattacks', *Council on Foreign Relation*s. (20 June 2017).

4.4 Lessons from the Alternative Policy

Similarly in the United States, mechanisms for sharing information have been a major element of policy about cybersecurity threats. Since effective sharing of information concerning risks is an important goal on both sides of the Atlantic, it makes sense to explore increased avenues of information sharing on a transnational basis.

The legal framework regarding cybersecurity in the United States is a matrix of federal and state laws, regulations, and policies—some applying horizontally across sectors and others aimed at specific government or private sectors.

4.4.1 Meeting the European Union's policy shortcomings

The United States and EU cybersecurity frameworks converge around risk assessment as the touchstone of effective cybersecurity. Assessment of information risk and measures tailored to risk is at the centre of the NIST Framework. It builds on risk assessment processes, is designed to integrate with existing risk management, and aims to provide a flexible and risk-based implementation that can be used in a variety of cybersecurity risk management processes.[187]

Despite its well-developed cybersecurity ecosystem, with the exception of a handful of state data security laws and regulations and certain specific sectoral provisions, United States federal law does not directly prescribe data security measures. Instead, the 2014 NIST Cybersecurity Framework[188] has become the keystone of U.S. cybersecurity risk management, influencing best practices and codes of conduct, regulation, litigation, auditing, and other elements of cybersecurity in the United States.

Therefore, the recent U.S. Commission on Enhancing Cybersecurity report recommended that the incoming administration "should build on the successes of the Cybersecurity Framework", finding that the framework "is playing an important role in strengthening risk management ecosystems" and "has tremendous value for organizations ... that are resource constrained and need an efficient and effective way to

[187] National Institute of Standards and Technology, (2018). *Cybersecurity Framework: Revised Version 1.1*, (April 16, 2018).
[188] National Institute of Standards and Technology, (2014). *Framework for Improving Critical Infrastructure Cybersecurity* (Version 1.0, 12 February 2014).

address cybersecurity risk".[189] NIST's central role in cybersecurity grew out of a 2013 executive order by President Obama that directed NIST to develop a set of standards, methodologies, procedures, and processes that would align with business and technology needs for cybersecurity and provide repeatable, cost-effective security measures consistent with voluntary international standards.[190] Over the following year, the first version of the framework was developed through extensive collaboration with industry, academic, and government stakeholders.[191]

Therefore, the NIST Framework avoids any set of specifications and explicitly disclaims a "one-size-fits-all" approach that could result in a tick-the-box exercise. Instead, the framework brings coherence to a wide array of existing international standards, guidelines, and practices by organising them into an analytical and organisational framework.[192] It is designed to enable organisations to evaluate their cybersecurity programs and preparedness by assessing their risk, objectives, and processes with a common taxonomy and mechanism. Though nominally aimed at critical infrastructure, the framework is specifically intended to be adaptable across a wide variety of organisations and sectors. It is "a living document" whose steps can be repeated to continuously improve cybersecurity. [193] The NIST Framework organises these standards and recommendations into three main parts: the Framework Core, the Framework Implementation Tiers, and the Framework Profile.[194]

Therefore, the Framework Core of the NIST is a set of actions, desired outcomes, and informative references that are common across organisations and technical standards. The Core is not a checklist of actions to perform nor a single standard.[195] Rather, it provides a conceptual framework for understanding common cybersecurity standards and practices. These offer organisations a means of mapping their approach to appropriate cybersecurity standards and best practices. The "functions" portion of the

---

[189] Commission on Enhancing National Cybersecurity, (2016). *Report on Securing and Growing the Digital Economy*. (1 December, 2016, p. 19).
[190] U.S. Government (2013). *Exec. Order No. 13636*, (78 Fed. Reg. 11737 at page 11741, 19 February 2013).
[191] National Institute of Standards and Technology, (2018). *Cybersecurity Framework FAQS Framework Basics*, [https://www.nist.gov/cyberframework/cybersecurity-framework-faqs-framework-basics]. (Accessed 23 January 2018).
[192] National Institute of Standards and Technology (2018). *Cybersecurity Framework: Revised Version 1.1*, (April 16, 2018).
[193] *Ibid.*
[194] *Ibid.*
[195] *Ibid.*

Framework Core categorises common cybersecurity activities at their broadest levels: identify, protect, detect, respond, and recover. The Framework Categories portion further subdivides the five functions into outcomes that are linked to an organisation's cybersecurity needs (such as asset management, access control, and detection processes).[196]

Therefore, the NIST Framework is easily adaptable to key elements of the NIS Directive. It provides a toolkit for organisations to adopt security measures that are (1) appropriate to the level of risk, (2) cost-effective, and (3) state of the art. The NIST Framework also embodies the consensus, private-sector-driven approach to standards development that — on both sides of the Atlantic — is enshrined in law and important to technology development. A common cybersecurity framework can bring the power of network effects to transatlantic cybersecurity protection.

Therefore, the transnational nature of the internet and cybersecurity threats requires transnational solutions. It is imperative that the EU and the United States speak the same language in terms of understanding each other's cybersecurity postures and responding to the global threats. Getting organisations to adopt effective security measures is essential to strengthening cybersecurity in general. This goal is central to the NIS Directive and to the European Commission and national cybersecurity policies.

Therefore, as wider adoption of the NIST Framework could increase understanding and uptake of cybersecurity measures based on widely accepted international standards. On the other hand, if businesses or industries have to adopt a unique cybersecurity framework for each European market in which they operate, they may choose, on cost and organisational grounds, to defer or to adopt suboptimal cybersecurity compliance for their EU-based operations. This could deteriorate the quality of cybersecurity across the EU.

4.5 The transatlantic partnership to enhance space security governance

Space-related cooperation is becoming an essential component of foreign policy planning and decision-making. The rationale for richer international cooperation in space

[196] National Institute of Standards and Technology (2018). *Cybersecurity Framework: Revised Version 1.1*, (April 16, 2018).

is more compelling than ever, given the long lead times of most space-related efforts. Moreover, cooperation of this kind helps reaffirm the principle of the peaceful use of outer space. To cooperate meaningfully, however, countries need to share a common appreciation of the value that a collective approach to space security brings versus a go-it-alone policy.

4.5.1 The EU as partners for space security

The relation between space and security has always been quite different in Europe as compared to that in other spacefaring nations. Contrary to most of them, the development of space activities in Europe has been mainly driven by civilian applications, which also means that space is relatively less used for security and defense purposes, despite the unique capabilities it offers. This situation has evolved in the past decade with the progress made in the European Security and Defence Policy (ESDP) and the new competences of the European Union over security and space matters. Space is called to support more and more European security actors in addressing all their security challenges. Furthermore, space is now fully integrated in the economy, and society is now relying on space for many critical services and policies. European citizens have thus become dependent on space infrastructures and services; hence they need to protect these and to ensure the sustainability of the space environment in order to maintain and to further develop all the benefits they derive from space. Europe has taken a leading role in political initiatives and technical activities to address this rising problem.

Therefore, space capabilities have been, and remain, an attribute of prestige and power for most nations. During the Cold War, space was an arena for competition between the U.S. and the USSR as each nation was trying to demonstrate its scientific and technical superiority. This dimension persists today as demonstrated, for instance, by the more recent development of the Chinese space activities. The development of space capabilities is also strongly linked to the development of military capabilities, since space and defense use the same technologies produced by the same industry, as illustrated by launchers and missiles. In contrast, space activities at European level have been mainly motivated by science and civilian applications, together with the will for an autonomous access to space.

Therefore, the investment in space for security and defense and its use in that context therefore remain limited compared to the other space powers. Thus, space programs for security and defense in Europe still remain to a great extent in the national realm, as they are mostly handled by member states at national or multilateral levels and do not benefit from European integration. This is still typically the case of the military space programs that are undertaken by a few European member states.

Therefore, the complexity of Europe can be both its asset and its liability. The asset is clear. No other region in the world has such significant experience in international cooperation as Europe does. The countries within the region cooperate multilaterally through alliances they are part of – mainly the European Union. The EU has a supranational power in many areas over its member states, which have mastered cooperation in order to achieve mutual goals and interests. In addition, the only existing international space agency in the world is in Europe – the European Space Agency (ESA), and it has proven that it is working for the benefits of all its members.

Therefore, one could assume that due to many examples of successful international/ regional cooperation Europe could be a leader on the international scene precisely for that reason – international cooperation. However, what has proven to work within the framework of intra-European cooperation, it is proving far more difficult to achieve on an international level with non-European partners – particularly on space security issues. In this regard, Europe does not speak with one voice. Due to a lack of coherent space governance in Europe, third countries often opt for bilateral cooperation with some individual European countries, ESA, or the EU. It is not unlikely that while partnership with one European entity might be challenging, it could be very successful with another.

Therefore, the implications of increasingly sophisticated counterspace systems in the hands of less-responsible actors are still to be addressed in Europe. At the same time, the EU is increasingly sensitive to this disparity in transatlantic treatment of international threats to a secure space environment, and accordingly, Brussels is seeking to play catch-up on this element of space security.

4.5.2 The U.S. as partners for space security

The U.S. space policy is elaborated within the executive branch of the U.S. government, under the authority of the President of the United States (POTUS). In the 21st century, three different President shaped the U.S. space policy and strategies: Presidents George W. Bush, Barack Obama, and Donald Trump, whom came up with three slightly different visions of space, their own agendas and priorities.

Therefore, the G.W. Bush administration space policy established overarching national policy that governed the conduct of U.S. space activities. The document emphasised security issues, encouraged private enterprise in space, and characterised the role of U.S. space diplomacy in terms of persuading other nations to support U.S. policy.[197] The Bush administration was also marked by the tragic events of 9/11 and the Second Gulf War, the so-called 'Second space war', which deepened the U.S. military reliance on space systems.[198] The operational and tactical advantages offered by space assets to its military, promoted the idea that the U.S. ought to take control of the so-called 'ultimate high-ground', which influenced Bush space policy at the time.

Therefore, the U.S. leadership in space remained the focus of the Obama administration (2009-2017), however, it renounced to the unilateral stance of the Bush administration.[199] Thus, the Obama policy underlined the need for international cooperation stating in its opening lines that "it is the shared interest of all nations to act responsibly in space to help prevent mishaps, misperceptions and mistrust."[200] Consistent with the Obama administration principles of security and cooperation, the United States wished to expand its international cooperation as a mean to foster its leadership in space-related fora and activities. The document is deliberately focused on the civil space applications, as well as on the use of space to promote national security.[201] The strategic vision for space elaborated by the Obama administration for the U.S. is still valid to date.

---

[197] Kaufman, M. (2006). 'Bush Sets Defense As Space Priority'. *The Washington Post*, (October 18, 2006).
[198] United States Department of Defense, (1992). 'The First Gulf War being the "First space War"'. *Report of the Secretary of Defense to the President and the Congress,* (Washington GPO, February 1992).
[199] Broad, W. & Chang, K. (2010). 'Obama Reverses Bush's Space Policy'. *The New York Times*, (June 28, 2010).
[200] U.S. Government, (2010). *National Space Policy of the United States of America*.
[201] *Ibid.*

Therefore, where the Obama administration distanced its space strategy from the Bush doctrine, the Trump administration brings them together in an 'America First', yet collaborative vision of space. The Trump administration has set objectives to its space policy that partly contradict those stated by the Obama administration (discontinuation of programmes, accent put on the military), however international cooperation is still explicitly encouraged.[202]

Therefore, in March, President Trump unveiled its National Space Strategy. The new strategy is meant to fit into an “America First” theme of the Trump administration, seeking to protect American interests in space through revised military space approaches and commercial regulatory reform.[203] The strategy features four “essential pillars” that constitute a whole-of-government approach to United States leadership in space, in close partnership with the private sector and allies. Three of those pillars are related to national security activities in space, including a shift to more resilient space architectures, strengthening deterrence and warfighting options in space, while the fourth pillar is devoted to developing “conducive” environments for working with commercial and international partners.[204]

Therefore the U.S. seeks to engage all spacefaring nations, including new space entrants, in discussions on some of the less politically sensitive space security challenges, such as orbital debris mitigation and remediation, behavioral space norms, and space sustainability. These discussions are mostly led by the Department of State. The U.S. is also trying to structure its dialogues with close allies to address some of the more sensitive space security challenges, including those that are defense- related. The Pentagon takes the lead here, in coordination with the State Department. While progress is being made toward a consensus on threats such as space debris, the often sensitive debates on man-made threats (e.g., counter-space) continue to prove challenging and remain somewhat underdeveloped. The public diplomacy dimension and the protection of privileged information are also vexing issues.

Therefore, adequate appreciation of the vulnerability of existing space assets and the priority attention that defending these assets deserve on the part of senior U.S. and

[202] U.S. Government, (2018). *National Space Strategy.*
[203] *Ibid.*
[204] *Ibid.*

allied policy-makers still appears to fall short of what is required. As a result, the U.S. is treading a fine line when seeking to align its domestic space security priorities with those of its allies. The reality that protective measures for space-related assets (including those that are ground-based) are necessary is generally accepted by all spacefaring nations and provides a useful starting point for policy-makers and security professionals within allied governments.

Therefore, the U.S. is leaning toward a view that, with the increasing number of space actors, collaboration with other countries, especially its allies, is the most prudent way to ensure space sustainability and protect its space assets over the long term. The dialogue, and some concrete action, has been mainly in the arena of nonmilitary threats to safe and secure space operations. Addressing potential adversary's temptation to disrupt or attack U.S. and allied space assets remains, understandably, compartmentalized. The future challenge for the U.S. will lie in the decision of how to expand collaboration without putting at risk sensitive information.

4.5.3 Bringing the transatlantic partnership on the international scene

The cyber threat issue is a major point of concern for the transatlantic partnership, and is extensively discussed through the North Atlantic Treaty Organisation (NATO) venue.[205] The EU and U.S. remain fully committed to European security and to the transatlantic partnership. Leaders in both the EU and United States have recognised that the interconnectedness of space and cyber domains, and the global nature of the threats demand international cooperation to tackle cyber security risks.[206]

Therefore, many of the regimes and mechanisms that have emerged from the United Nations (UN) bodies and from alternative forums fall under the heading of "soft law." It can be said to be fairly successful in that it coordinates all of these activities and the centralized sharing of information. However, it is also entirely dependent upon the cooperation of States. It is, therefore, a limited proactive instrument of global space governance. Nonetheless, they do represent a clear global political view, and the vote

[205] Schmitt, et al. (2013). T*allinn Manual on the International Law Applicable to Cyber Warfare*. CCDCOE. (Cambridge University Press: 2013).

[206] Meola, A. (2016). 'Cyber attacks against our critical infrastructure are likely to increase', *Business Insider*, (26 May 2016).

count can often indicate where specific States stand on any given issue. In its early years, General Assembly resolutions were a successful instrument of global governance in general and space governance in particular. However, as issues have become more complex, General Assembly resolutions have become less effective.

Therefore, if international cooperation will be crucial, the dialogue in developing a cybersecurity framework through UN structures seems unfit. Indeed, the UN system is struggling to develop a comprehensive multilateral cyber policy. Cyber security is a very broad concept, and the various UN organizations have a limited understanding of the issues related to it and their own relevant responsibilities.[207]

Therefore, where the international community is slow to come up with clear norms and incentive mechanisms to apply these norms, national legislation may push this frontier.[208] The regional space regimes are also valuable as an outreach instrument for the global regimes to attain their policy goals, implement the global norms and regulations because of its physical proximity to the targeted countries and regions. These regional outreach mechanisms are considered to bridge the top-down gap between the global, regional and national levels and can facilitate the bottom-up feedback flow in such vertical global-regional-national policy-regulation lifting.[209]

Therefore, the NIST Framework and the European Cybersecurity Toolbox— as risk-based taxonomy of standards and practices set out using common cyber-risk-management language — could provide a blueprint on which governments, businesses, and other stakeholders can build strong base for cybersecurity for Outer Space. Thus, the transatlantic partnership in security remain strong and indispensable as the U.S. and Europe are at their greatest when their partnership are strong.[210]

Therefore, there is no doubt that the EU has a vested interest in space security, and through a growing variety of its space activities and a unique diplomatic network, the EU is uniquely positioned to be in the forefront of global endeavours supporting responsible behaviour in space. In 2008, responding to a UN call for transparency and

---

[207] Baseley-Walker, B. (2014). 'The UN Structure: The Intersection of Cyber Security and Outer Space Security', *Chatham House*, (December 2014, p.48).
[208] Jakhu, R. & Pelton, J. (2017). "Introduction to the Study on Global Space Governance", *Global Space Governance: An International Study*, (Eds Ram S. Jakhu, p.51).
[209] Liao, X. (2016). 'The Space Regionalisation and Global Space Governance', *Yearbook on Space Policy 2014.* (C. Al-Ekabi et al. (eds.), Springer-Verlag Wien, p.195-196).
[210] European Parliament & US House of Representatives (2017). 'Joint Statement', *81st Inter-Parliamentary Meeting Transatlantic Legislators' Dialogue*, (Washington Dc, 5 December 2017).

confidence building measures in space, the EU has published its first draft of Code of Conduct for Outer (ICoC) for Space Activities. Its main purpose was to create a global norm of responsible behaviour in space as well as to pave the way for enhanced international cooperation mechanisms.[211] Thus, a large majority of states outside Europe were sceptical of the ICoC, as for most states, what the code contained was not so much an issue as much as the process, because many of the even established spacefaring powers were not part of the process that developed the code. This factor seriously impeded progress on the ICoC with many viewing the EU effort as presumptuous.[212] Thus, the effectiveness of the implementation of coordinated European actions will depend on the ability to achieve maximum synergy within a coherent European effort among intergovernmental and communitarian actors but also with national actors, who remain the main players in this field.

Therefore, it is important to remember that space security issues can be politically very sensitive. Hence, spacefaring nations such as the United States, China, or Russia will often have a hard time to lead an international space security initiative regardless of how good it might be due to certain political implications that would go along with these countries leading it. Europe, on the other hand, is different and a unique as it can be a broker between the traditional Eastern and Western powers. It is situated right in the middle, and it alone is comprised of many countries, which would often mean that it already represents a sort of an international view, which can be a lot more neutral in comparison to the countries mentioned above.

Therefore, the EU in that regard lost an opportunity to connect with the non-European space powers because having the non-European bloc support for such an initiative could have been significant. Asia, Africa and Latin America are important in this regard because newer space powers are going to be coming from these regions, and not from Europe. Hence, there is a need to have these countries on board, without which one may end with an instrument that may have a significant number of countries but the critical players that will make a difference stay outside. Europe and the West in general need to acknowledge that it is in these regions that new challenges are going to be

[211] Pindják, P. (2016). "A Stronger EU in Cosmos: Embracing the Concept of Space Security", *INCAS BULLETIN*, (Volume 8, Issue 3).

[212] Rajagopalan, R. (2016). "The International Code of Conduct and Space Sustainability", *Yearbook on Space Policy 2014.* (C. Al-Ekabi et al. (eds.), Springer-Verlag Wien, p.237).

coming from. So far, when it comes to space, Europe hasn't played that role too successfully, but opportunity is still out there if carefully approached.

Moreover, The overall international space context is changing fast: competition is increasing; new entrants are bringing challenges and new ambitions in space; space activities are becoming increasingly commercial with greater private sector involvement; and major technological shifts are disrupting traditional industrial and business models in the sector, reducing the cost of accessing and using space.[213] Thus, on the international scene, the emergence of new actors and technologies has created its own dynamics, making the outer space not only crowded but also making the process of tracking and detection of attacks more difficult.[214]

Therefore, if cyber security threats to satellite communications are a relatively new phenomenon, they have quickly come to the forefront of concern for the sustainability of satellite systems due to the vulnerabilities that such threats may exploit and negatively impact.[215] Thus, a flexible regime would avoid the inevitable delays in agreement and implementation associated with any regulated, centralised and directive approach developed by an international body like the United Nations. Building from the transatlantic cooperation and the policies already in place, a new regime would provide a practical leadership in delivering enhanced security within the whole of the global space sector. Finally, it would develop established and trusted connections with the space and cyber communities, including government agencies, academia and industrial concerns worldwide.

[213] European Commission, (2016). "Space Strategy for Europe", *Communication from the commission to the European parliament, the council, the European economic and social committee and the committee of the regions*.
[214] Rajagopalan, R. (2016). 'The International Code of Conduct and Space Sustainability', *Yearbook on Space Policy 2014*. (C. Al-Ekabi et al. (eds.), Springer-Verlag Wien, p.229-230).
[215] Housen-Couriel , D. (2016). 'Cybersecurity threats to satellite communications: Towards a typology of state actor responses', *Acta Astronautica, (*Issue 128*,* p.409).

Conclusion

In contrast to the Cold War period, the space environment today involves some 60 countries and government consortia with different strategic objectives and levels of economic and technological development.[216] Space capabilities today offer a wide spectrum of critical civilian, commercial, and military-related applications, services, and benefits to a wide spectrum of users. There are also many commercial satellite operators. Earth observation, communications, and satellite navigation, originally supporting mainly military activities, are now part of day-to-day civilian and commercial life. As a result, there is a growing concern regarding how best to preserve safe, stable, and sustainable space operations over the long term. A growing concern to the security of the space infrastructure is posed by cyber vulnerabilities at the junction of space.

Therefore, the awareness of the damaging impact of cyber-attacks is growing globally, and it is important to take into account that cyber security is not only a matter of technical measures, but also of high politics. Europe and the United States, as the major capable space powers, are uniquely vulnerable, and need to address the issue. However, the current political set addressing the purposeful cyber attacks on space systems is slim.

Moreover, the issues related to space and cyber security are closely linked to the international political and strategic context. as only state actors (or state-supported ones) have enough financial and human capacity to invest in developing the most powerful cyber weapons. Cyber-attacks can have a background in international relations, or bring about the consequences that can escalate to a political and diplomatic level. Unfortunately, however, efforts to contain aggressive behaviour of states in cyberspace, by developing international norm-setting through the United Nations, have failed.

Therefore, in 2017, the Council of the European Union agreed to develop the cyber diplomatic toolbox, a joint EU diplomatic response to deter malicious cyber operations.In this international context, the EU cyber diplomatic toolbox relies on the assumption that

[216] Schulte GL (2012). 'Protecting global security in space'. *Presentation at the S. Rajaratnam School of International Studies Nanyang Technological University*, [http:// www.defense.gov/home/features/2011/0111_nsss/docs/Rajaratnam%20School%20of%20 International%20Studies%20on%20Protecting%20Global%20Security%20in%20Space,%20May %209,%202012.pdf]. (Singapore, 9 May 2012).

international law is applicable to cyberspace, and that states should not conduct or support any cyber attack emanating from their territories contrary to their international obligations. With the cyber diplomatic toolbox, the EU and its member states try to draw a red line for acceptable behavior in cyberspace and to alter adversaries' calculus when deploying cyber operations. However, the toolbox has to be considered in is the combination of all the cyber security policy measures applicable for the space domain, and ultimately, addressing the cyber security threats and risks represent a systemic challenge to all space-faring nations, that is only viable if the full set of agencies and organisations would work together in a synergistic and complementary manner.

There is therefore a growing need to reach a consensus on additional political actions directly applicable to the conduct of cyber conflict. This will require political will, close cooperation, and greater trust between the major space powers, so as to lessen the chances of a conflagration involving space assets, with all of the negative and unknown consequences that this would entail. To this end, to combine the political set of provision of the European Union and the United States seems a valuable option, and would follow Lewis and Livingstone recommendation to build an international 'community of the willing' to develop a space cybersecurity regime competent to match the range of threats. [217]

Therefore, cooperation is embedded in a long-term strategy, it becomes more efficient as a set of protocols and unwritten rules govern these political practices and assistance procedures, and the European Union and the United States are at the forefront in this regard. As cooperation is improved, so is information-sharing and the capacity to respond quickly attacks. Thus, a unified approach can produce "network effects" — thereby strengthening cybersecurity across the EU, and throughout the international scene. Thus, more study needs to be done on the transatlantic partnership, as to answer which venue would be best suited to bring and develop the concern on the international scene.

[217] Livingstone, D. & Lewis, P. (2016). 'Space, the Final Frontier for Cybersecurity?', *Chatham House Research Paper*.

References

Algieri, F. and Kammel, A. (2010). 'Anmerkungen zum ersten Jahrzehnt der ESVP', *Strategie und Sicherheit*, (Volume 2010, Issue 1, Pages 61–72)

Aliberti, M. & Krasner, S. (2016). "Governance in Space", *Yearbook on Space Policy 2014*. (C. Al-Ekabi et al. (eds.), Springer-Verlag Wien, p.145)

Asbeck, F. (2014). 'An EU View: Comparisons and Establishing Norms in the Cyber and Space Domains', *Chatham House working paper*, (December 2014, p.42)

Bardin, J. (2014). "Satellite Cyber Attack Search", *Cyber Security and IT Infrastructure Protection*, (Elsevier Inc, p.317)

Bardach, E. et al. (2016). *A Practical Guide for Policy Analysis: The Eightfold Path to More Effective Problem Solving.* (Sage Publication: 2016, Fifth Edition)

Baseley-Walker, B. (2014). 'The UN Structure: The Intersection of Cyber Security and Outer Space Security', *Chatham House*, (December 2014, p.48)

Baylon, C. (2014). "Challenges at the Intersection of Cyber Security and Space Security: Country and International Institution Perspectives", *Chatham House*, (December 2014)

Bennett, C. (2015). 'Kremlin's ties to Russian cyber gangs sow US concerns', *The Hill*, (10 November 2015)

Bowen, G. A. (2009). 'Document analysis as a qualitative research method'. *Qualitative Research Journal*, 9(2), 27-40

Broad, W. & Chang, K. (2010). 'Obama Reverses Bush's Space Policy'. *The New York Times*, (June 28, 2010)

CCDCOE (2013). *NATO's Tallinn Manual*, (Cambridge University Press)

Clark, C. (2016). "Cyber Attack On Satellite Could Be Act Of War: HPSCI Ranking", *Breaking Defense*, (May 4, 2017)

Clapper, J. (2015). 'Worldwide Threat Assessment of the US Intelligence Community', *Statement for the Record. Senate Armed Services Committee*, (February 26, 2015)

Commission on Enhancing National Cybersecurity, (2016). *Report on Securing and Growing the Digital Economy*. (1 December, 2016, p. 19)

Consultative Committee for Space Data Systems, (2015). 'Security Threats Against Space Missions', *Report Concerning Space Data System Standards*, (CCDS 350 1-G-2, December, 2015)

Council of the European Union (2017). *Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities* ("Cyber Diplomacy Toolbox"). (Brussels, 7 June 2017)

Csernatoni, R. (2016). 'Time to Catch Up: The EU's Cyber Security Strategy', *European Public Affairs*, (March 4, 2016)

Department of Homeland Security (DHS), (2018). *'Critical infrastructure sectors' on the Department of Homeland Security of the United States*, [https://www.dhs.gov/critical-infrastructure-sectors]

De Zan, T. (2017). 'Deterring "bad hombres": the EU cyber diplomatic toolbox', *Italian Institute for International Security Policy*, (October 20, 2017)

Director General's Office, (2012). 'EBU Deplores Middle East Satellite Jamming', EBU: [https://www.ebu.ch/contents/news/2012/10/ebu- deplores-middle-east-satelli.html], (October 22, 2012)

Elgin, B. (2008). "Network Security Breaches Plague NASA", *Bloomberg*, (20 November 2008)

European Union – External Action (2014). *Strategic Notes*, (26 March 2014)

European Parliament, (2016). *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*. (Brussels, July 2016)

European Commission (2017). 'Building an Effective European Cyber Shield: Taking EU Cooperation to the Next Level'. *EPSC Strategic Notes*, (Issue 24, 8 May 2017)

European Parliament, (2007). *Taking forward the European Space Policy*, (COM(2007) 212)

European Commission (2017). 'Building an Effective European Cyber Shield', *Strategic Notes*, (Issue 24, 8 May 2017)

European Parliament, (2008). *Space and security*, (2008/2030(INI))

European Union External Action, (1990). *Transatlantic Agenda*

European Union for Foreign Affairs and Security, (2013). *The Cybersecurity Strategy of the European Union – An Open, Safe and Secure Cyberspace*. JointCOM(2013) 1 Final. (Brussel, February 7, 2013)

European Commission (2016). 'Fact Sheet: FAQ: Joint Framework on countering hybrid threats', *Strategic Notes*, (6 April 2016)

European Parliament & US House of Representatives (2017). 'Joint Statement', *81st Inter-Parliamentary Meeting Transatlantic Legislators' Dialogue*, (Washington Dc, 5 December 2017).

European Parliament, (2009). *Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community* (OJ C 306, 17.12.2007); (entry into force on 1 December 2009)

European Commission, (2016). *Space Strategy for Europe*. (COM(2016) 705 final)

European Commission. (2013). "Impact assessment", *Proposal for a Directive of the European Parliament and of the Council Concerning measures to ensure a high level of network and information security across the Union*. (SWD(2013) 32 final, p.25).

Eutelsat, (2013). 'Satellite Interference: an Operator's Perspective', *ITU*: [https://www.itu.int/en/ITU-R/space/workshops/2013-interference-geneva/presentations/Ethan%20Lavan%20-%20Eutelsat.pdf], (June 10, 2013)

Federal Communications Commission, (2018). 'Jammer Enforcement', *FCC*, [https://www.fcc.gov/general/jammer-enforcement]

Foxall, A., 'Putin's Cyberwar: Russia's Statecraft in the Fifth Domain', *Russia Studies Centre*, (Policy Paper No. 9, May 2016)

Gallagher, N. (2010). "Space Governance and International Cooperation", *Astropolitics*, 8:2-3

Geers, K. (2015), *Cyber War in Perspective: Russian Aggression against Ukraine*, (Tallinn: NATO CCD COE, p. 20)

Gini, A. (2014). 'Cyber Crime - From Cyber Space to Outer Space', *Space Safety Magazin*e, (February 14, 2014)

Goldstein J, and Keohane R. (1993). *Ideas and foreign policy. Beliefs, institutions, and political change*. (Cornell University Press, Ithaca)

Grieco J. (1988). *Anarchy and the limits of cooperation - A realist critique of the newest liberal institutionalism*. (Int Organ 42:485–507)

Grisham, P. (2017). "Satellite Cybersecurity and Information Assurance: How Secure Are Our Nation's Satellites?", *Keynotes from CompTIA webinar,* (March 1, 2017)

Hambling, D. (2017). 'Ships fooled in GPS spoofing attack suggest Russian cyberweapon', *New Scientist*, [https://www.newscientist.com/article/2143499-ships-fooled-in-gps-spoofing-attack-suggest-russian-cyberweapon/], (2017, August 10)

Hardin, G. (1968). 'The Tragedy of the Commons', *Science*, (13 Dec 1968: Vol. 162, Issue 3859, pp. 1243-1248)

Harrison, R. (2013). 'Unpacking the Three C's: Congested, Competitive, and Contested Space', *Astropolitics* (11(3):123-131, September 2013)

Harrison R., el al. (2009). *Space deterrence: the delicate balance of risk.*

Harrison, R. (2015). 'The Role of Space in Deterrence', *Handbook of Space Security*, (Kai-Uwe Schrogl & al., eds., Springer)

Hasenclever A., Mayer P., and Rittberger V. (2002). *Theories of international regimes*. (Cambridge University Press, Cambridge)

Hays, P. (2015). "Defining Space Security ", *Handbook of Space Security*. (Springer Science+Business Media New York, p.3-7)

Hesse, M. and Hornung, M (2015). 'Space as a Critical Infrastructure', *Handbook of Space Security*. (K.-U. Schrogl et al. (eds.), Springer Science+Business Media New York)

Hogg, C. (2004). 'HK probes Falun Gong 'hacking', *BBC News*, [http://news.bbc.co.uk/2/hi/asia-pacific/4034209.stm], (November 23, 2004)

Housen-Couriel , D. (2016). 'Cybersecurity threats to satellite communications: Towards a typology of state actor responses', *Acta Astronautica*, (Issue 128, p.409)

International Astronomical Association, (2017). *Space Traffic Management: Towards a Roadmap for implementation, IAA Cosmic Study* (2017:80)

International Telecommunication Union, (2016). *Measuring the Information Society Report 2016*

International Telecommunication Union, (2017). 'About GCA', Global Cybersecurity Agenda (GCA), [https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx]. (Accessed November 12, 2017)

Jakhu, S. (2013). 'Satellites: Unintentional and Intentional Interference', *Secure World Foundation*. (June 17, 2013)

Jakhu, R. & Pelton, J. (2017). "Introduction to the Study on Global Space Governance", *Global Space Governance: An International Study*, (Eds Ram S. Jakhu, p.51)

Joint Chiefs of Staff, (2013). 'Cyberspace Operations', Joint Publication (JP) 3-12 (R), *Cyberspace Operations*, (5 February 2013, v-vi and I-2)

Kaufman, M. (2006). 'Bush Sets Defense As Space Priority'. *The Washington Post*, (October 18, 2006)

Keohane R. (1984). *After hegemony. Cooperation and discord in the world political economy.*
(Princeton University Press, Princeton)

Keohane R. (1989). Neoliberal institutionalism. A perspective on world politics, *International institutions and state power. Essays in international relations theory*. (Westview Press, Boulder, pp 1–20)

Landler, M. & Markoff, J. (2007). "Digital Fears Emerge After Data Siege in Estonia", *New York Times*, (May 29, 2007)

Livingstone, D. & Lewis, P. (2016). 'Space, the Final Frontier for Cybersecurity?',
Chatham House Research Paper

Liao, X. (2016). 'The Space Regionalisation and Global Space Governance', *Yearbook on Space Policy 2014*. (C. Al-Ekabi et al. (eds.), Springer-Verlag Wien, p.195-196)

Limnell, J. et al. (2017). 'EU cyber diplomacy requires more commitment, *EU Observer*, (July 7, 2017)

Lipton, E., et al. (2016). 'The Perfect Weapon: How Russian Cyberpower Invaded the U.S.', *The New York Times*, (13 December 2017)

Lu, M. (2014). ‘Types of Cyber Attacks’, *TCIPG*, (September 12, 2014)

McCoy, J. (2007). ‘Intelsat Shuts Down Transponder Hijacked By Terrorists’, *Via Satellite*: [http://www.satellitetoday.com/uncategorized/2007/04/26/intelsat-shuts-down-transponder-hijacked-by-terrorists/]. (April 26, 2007). (Accessed November 13, 2017)

MacRae, D. & Wilde, J. (1979). *Policy analysis for public decisions*. (Duxbury Press, 1979)

Martinez, P. (2015). ‘Space Sustainability’, *Handbook of Space Security*. (Springer Science+Business Media New York)

Mayence J-F (2010). ‘Space security: transatlantic approach to space governance’, *Prospects for transparency and confidence-building measures in space*. (ESPI, Vienna, p 35)

Meola, A. (2016). ‘Cyber attacks against our critical infrastructure are likely to increase’, *Business Insider*, (26 May 2016)

Moltz, J. (2010) "Space and Strategy: A Conceptual versus Policy Analysis", *Astropolitics, 8:2-3*

Moravcsik A. (1997). *Taking preferences seriously - A liberal theory of international politics*. (IntOrgan 51:513–553)

Mutschler, M. (2015). ‘Security Cooperation in Space and International Relations Theory’, *Handbook of Space Security*. (K.-U. Schrogl et al. (eds.), Springer Science+Business Media New York)

Naja, G & Mathieu, C. (2015). "Space and Security in Europe", Handbook of Space Security, (K.-U. Schrogl et al. (eds.),. Springer Science +Business Media New York, p.377)

Nakashima, E. (2015). ‘Russian hacker group exploits satellites to steal data, hide tracks’, *The Washington Post*, (September 9, 2015)

National Counterintelligence and Security Center (2014). *National Counterintelligence Strategy of the United States*

National Institute of Standards and Technology, (2004). *Standards for Security Categorization of Federal Information and Information Systems.* (FIPS PUB 199)

National Institute of Standards and Technology, (2012). *Guide for Conducting Risk Assessments*, (NIST SP 800-30 Rev. 1, September 2012)

National Institute of Standards and Technology, (2018). *Cybersecurity Framework FAQS Framework Basics*, [https://www.nist.gov/cyberframework/cybersecurity-framework-faqs-framework-basics]

National Institute of Standards and Technology, (2014). *Framework for Improving Critical Infrastructure Cybersecurity* (Version 1.0, 12 February 2014)

National Institute of Standards and Technology, (2018). *Cybersecurity Framework: Revised Version 1.1*, (April 16, 2018)

National Institute of Security and Technology, (2018). 'Advanced Persistent Threat'. *NIST SP 800-39*, [csrc.nist.gov/Glossary/?term=2856]

National Research Council, (1995). *The Global Positioning System: A shared National Asset*. (Washington, DC: The National Academies Press,1995)

Nebehay, S. (2010). 'U.N. tells Iran to end Eutelsat satellite jamming', *Reuters*: [https://www.reuters.com/article/us-iran-jamming-itu/u-n-tells-iran-to-end-eutelsat-satellite-jamming-idUSTRE62P21G20100326], (March 26, 2010)

Pasco, X. (2015). 'Various Threats of Space Systems', *Handbook of Space Security*, (Kai-Uwe Schrogl & al., eds., Springer, p. 673-674)

Patton, C. et al. (2013). *Basic Methods of Policy Analysis and Planning*. (Taylor and Francis: 2013, 3rd Edition)

Pellegrino, M., & Stang, G. (2016). *Space security for Europe*. (Paris: European Union Institute for Security Studies)

Pelton, J. et al. (2015). 'Space Safety', *Handbook of Space Security*. (K.-U. Schrogl et al. (eds.), Springer Science+Business Media New York)

Pindják, P. (2016). "A Stronger EU in Cosmos: Embracing the Concept of Space Security", *INCAS BULLETIN*, (Volume 8, Issue 3)

Pomerleau, M. (2016). 'Threat from Russian UAV Jamming Real, Officials Say', *C4ISRNET*, (Dec 20, 2016)

PwC (2018). *Dependence of the European Economy on Space Infrastructures,: Potential impacts of space assets loss*. (EU publications, February 2018)

Kaufman, M. (2006). 'Bush Sets Defense As Space Priority'. *The Washington Post*, (October 18, 2006)

Rajagopalan, R. (2016). "The International Code of Conduct and Space Sustainability", *Yearbook on Space Policy 2014.* (C. Al-Ekabi et al. (eds.), Springer-Verlag Wien, p.232)

Remuss, N. (2015). 'Responsive Space', *Handbook of Space Security,* (K.-U. Schrogl et al. (eds.),. Springer Science +Business Media New York)

Robinson, J. (2016). "Governance challenges at the intersection of space and cyber security". *The Space Review*, (February 15, 2016)

Robinson , J. (2017). 'Deterring Chinese and Russian space hybrid warfare by economic and financial means', *The Space Review*, (September 18, 2017)

Risse-Kappen T. (1994). *Ideas do not float freely - Transnational coalitions, domestic structures, and the end of the cold war.* (Int Organ 48:185–214)

Sadeh, E. (2015). "Obstacles to International Space Governance", *Handbook of Space Security*, (K.-U. Schrogl et al. (eds.),. Springer Science+Business Media New York, p.24)

Secure World Foundation, (2015). *Strategic Stability and Space,* (Washington DC: 2015)

Segal, A. (2017). 'EU Creates a Diplomatic Toolbox to Deter Cyberattacks', *Council on Foreign Relations*. (20 June 2017)

Schmitt, et al. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. (Cambridge University Press: 2013)

Schulte GL (2012). 'Protecting global security in space'. *Presentation at the S. Rajaratnam School of International Studies Nanyang Technological University*, (Singapore, 9 May 2012)

Sgobbi, D. et al. (2015). 'Space and Cyber Security', *Handbook of Space Security,* (K.-U. Schrogl et al. (eds.),. Springer Science +Business Media New York)

Sheehan, M. (2009). *Securing Outer Space*, (Routledge: NY)

Sheehan, M. (2015). "Defining Space Security ", *Handbook of Space Security*. (Springer Science+Business Media New York, p.17-18)

Space Security Index (2013). *Space Security Index 2013*, (Eds.Cesar Jaramillo, Ontario: June 2013)

Space Security Index (2017). *Space Security Index 2017*, (Eds. Jessica West, Ontario: May 2017)

Suzuki, K. (2016). "How Governance Models Affect Geopolitics: The Asian Case Study", *Yearbook on Space Policy 2014*. (C. Al-Ekabi et al. (eds.), Springer-Verlag Wien, p.199)

Talleur, T. (1999). *Russian Domain Attacks Against NASA Network Systems*, (Inspector General's Office, NASA)

Tanase, S. (2015). 'Satellite Turla: APT Command and Control in the Sky', *Kaspersky Lab*, (Sept. 9, 2015)

UK HM Government (2014). *National Space Security Policy*, (UKSA/13/1292, p. 2)

United States Department of Defense, (1992). 'The First Gulf War being the "First space War"'. *Report of the Secretary of Defense to the President and the Congress*, (Washington GPO, February 1992)

U.S. Government, (2010). *National Space Policy of the United States of America*

U.S. Department of Defense and the Office of the Director of National Intelligence, (2011). *National Security Space Strategy*. (Washington, D.C., January 2011)

U.S. Government (2013). *Exec. Order No. 1363*6, (78 Fed. Reg. 11737 at page 11741, 19 February 2013)

U.S. Government, (2018). *National Space Strategy*.

U.S. Government Printing Office (2011). *Report to Congress of the U.S.-China Economic and Security Review Commission*, (pp. 215–217)

Van Impe, K. (2017). 'Simplifying Risk Management'. *Security Intelligence*, (IBM, March 28, 2017)

Weeden, B. & Chow, T. (2015). "Developing a framework and potential policies for space sustainability based on sustainable management of common-pool resources", *Secure World Foundation*

Waltz, K. (1979). *Theory of international politics*. (Random House, New York)

Waltz K. (1959). *Man, the state and war*. (Columbia University Press, New York)

Weimer, D. et al. (2017). *Policy Analysis: Concepts and Practice*. (Routledge: 2017)

CHARLES UNIVERSITY

MSc International Security, Intelligence and Strategic Studies

2017-2019

Dissertation Archive Permission Form

I do not give the School of Social and Political Sciences, University of Glasgow permission to archive an e-copy/soft-bound copy of my MSc dissertation in a publicly available folder and to use it for educational purposes in the future.

Student Name (BLOCK LETTERS): LISA PERRICHON

Student Number: 2272775

Student Signature: LISA PERRICHON

Date: 29 MAY 2018

PLEASE INCLUDE A COPY OF THIS FORM WITH THE SUBMITTED SOFT-BOUND COPY OF YOUR DISSERTATION.