Keele
University

The security of the European Union’s critical outer space infrastructures

Phillip A. Slann

Thesis submitted for the degree of Doctor of Philosophy in International Relations

March 2015

Keele University

Abstract

This thesis investigates the European Union's (EU) conceptualisation of outer space security in the absence of clear borders or boundaries. In doing so, it analyses the means the EU undertakes to secure the space segments of its critical outer space infrastructures and the services they provide. The original contribution to knowledge offered by this thesis is the framing of European outer space security as predicated upon anticipatory mechanisms targeted towards critical outer space infrastructures. The objective of this thesis is to contribute to astropolitical literature through an analysis of the EU's efforts to secure the space segments of its critical outer space infrastructures, alongside a conceptualisation of outer space security based upon actor-specific threats, critical infrastructures and anticipatory security measures. The EU's Galileo and Copernicus programmes are identified as future critical outer space infrastructures through their services' expected contributions to EU-level policy-multiplication and European states and societies, making them examples of regional and global European space power projection.

Following the designation of the Galileo and Copernicus programmes as critical outer space infrastructures, the thesis details the dangers and risks, both intentional and environmental, which the EU has publicly acknowledged as being the most threatening. Although the specific risk assessments for the Galileo and Copernicus projects are confidential, the generic dangers and risks for satellites in Lower Earth Orbit and Middle Earth Orbit referred to in EU policy documents are explored, including space debris, space weather phenomena, orbital congestion and the possibility of the future weaponisation of near-Earth space.

At a macro-level, the EU’s determination to mitigate both intentional and environmental risks through international diplomacy, improved satellite design and increased awareness of near-Earth space are analysed as being reflective of preventive and preemptive forms of anticipatory security. On a micro-level the EU’s efforts to protect its outer space infrastructures from said risks are framed within the context of critical infrastructure security.

Table of contents

Figures and images

Abbreviations

ABL	-	Airborne Laser
ABM	-	Anti-Ballistic Missile
ACE	-	Advanced Composition Explorer
AFWA	-	Air Force Weather Agency
ALBM	-	Air-Launched Ballistic Missile
ALMV	-	Air-Launched Miniature Vehicle
Ariane 5 ME	-	Ariane 5 Mid-life Evolution
ASAT	-	Anti-Satellite
ASI	-	Agenzia Spaziale Italiana
ATM	-	Air Traffic Management
BMD	-	Ballistic Missile Defence
CAM	-	Collision Avoidance Manoeuvre
CCSDS	-	Consultative Committee for Space Data Systems
CD	-	Conference on Disarmament
CERN	-	Organisation Européenne pour la Recherche Nucléaire
CFSP	-	Common Foreign and Security Policy
CIIP	-	Critical Information Infrastructure Protection
CIP	-	Critical Infrastructure Protection
CIR	-	Critical Infrastructure Resilience
CME	-	Coronal Mass Ejection
CNES	-	Centre National d’Études Spatiales
CNSA	-	Chinese National Space Administration
COIL	-	Chemical Oxygen-Iodine Laser
COSPAS-SARSAT	-	Cosmicheskaya Sistyema Poiska Avariynich Sudov- Search

		and Rescue Satellite-Aided Tracking
CSA	-	Canadian Space Agency
CSEISSWE	-	Committee on the Societal and Economic Impacts of Severe Space Weather Events: A Workshop
DEW	-	Directed-Energy Weapons
DLR	-	Deutches Zentrum für Luft- und Raumfarht e. V.
DODI	-	Department of Defense Instruction
EC	-	European Commission
ECI	-	European Critical Infrastructure
EDA	-	European Defence Agency
EGNOS	-	European Geostationary Satellite Overlay Service
ELDO	-	European Launcher Development Organisation
EMP	-	Electromagnetic Pulse
EPCIP	-	European Programme for Critical Infrastructure Protection
ERNO	-	Entwicklungsring Nord
ERS	-	European Remote Sensing
ESA	-	European Space Agency
ESDP	-	European Spatial Development Perspective
ESP	-	European Space Policy
ESPI	-	European Space Policy Institute
ESRIN	-	European Space Research Institute
ESRO	-	European Space Research Organisation
EU	-	European Union
EUMETSAT	-	European Organisation for the Exploitation of Meteorological Satellites

Eurocontrol	-	European Organisation for the Safety of Air Navigation
FOC	-	Fully Operational Capability
FP7	-	Seventh Framework Programme for Research
FY-1C	-	Fen-Yung 1C
G-MOSAIC	-	GMES services for Management of Operations, Situation Awareness and Intelligence for regional Crises
GBAS	-	Ground-Based Augmentation System
GEO	-	Geosynchronous Orbit
GIOVE	-	Galileo In-Orbit Validation Element
GISC	-	GMES In-Situ Coordination
GLONASS	-	Globalnaya Navigatsionnaya Sputnikovaya Sistema
GMES	-	Global Monitoring for Environment and Security
GNSS	-	Global Navigation Satellite System
GOCE	-	Gravity field and Ocean Circulation Explorer
GOES	-	Geostationary Operational Environmental Satellite
GPS	-	Global Positioning System
GRAVES	-	Grand Résau Adapté à la Veille Spatiale
GSA	-	European Global Navigation Satellite System Authority
GSO	-	Geostationary Orbit
HEO	-	Higher Earth Orbit
IADC	-	Inter-Agency Space Debris Coordination Committee
ICBM	-	Inter-Continental Ballistic Missile
IncREO	-	Increasing Resilience through Earth Observation
INPE	-	Instituto Nacional de Pesquisas Espaciais
INW	-	Isotropic Nuclear Weapons

IOV	-	In-Orbit Validation
IRBM	-	Intermediate Range Ballistic Missile
ISS	-	International Space Station
IT	-	Information Technology
ITU	-	International Telecommunications Union
JAXA	-	Japan Aerospace Exploration Agency
JCF	-	Joint Forces Commander
JDAM	-	Joint Direct Attack Munition
JP3-14	-	Joint Publication 3-14
KEW	-	Kinetic-Energy Weapons
L1	-	Lagrange Point 1
LEO	-	Lower Earth Orbit
LF/HC	-	Low Frequency/High Consequence
LTS	-	Large Technical System
MDGPS	-	Maritime Differential Global Positioning System
MEO	-	Middle Earth Orbit
MFF	-	Multi-annual Financial Framework
MHV	-	Miniature Homing Vehicle
MIRACL	-	Mid-Infrared Advanced Chemical Laser
MSAS	-	Multi-transport Satellite-based Augmentation System
MUSIS	-	Multinational Space-based Imagery System
NASA	-	National Aeronautics and Space Administration
NATO	-	North Atlantic Treaty Organisation
NOAA	-	National Oceanic and Atmospheric Administration
NOTAM	-	Notice to Airmen

NRO	-	National Reconnaissance Office
NSC	-	National Security Council
Ofcom	-	Office of Communications
ORFEO	-	Optical and Radar Federated Earth Observation
OST	-	Outer Space Treaty
PAROS	-	Prevention of an Arms Race in Outer Space
PCCIP	-	President’s Commission on Critical Infrastructure Protection
PEO	-	Polar Elliptical Orbit
POES	-	Polar Operational Environmental Satellite
PRC	-	People’s Republic of China
PRS	-	Public Regulated Service
PPWT	-	Treaty on Prevention of the Placement of Weapons in Outer Space and the Threat or Use of Force against Outer Space Objects
RAF	-	Royal Air Force
RFSA	-	Russian Federal Space Agency
SAR	-	Search And Rescue
SBAS	-	Satellite Based Augmentation System
SBL	-	Space-Based Laser
SBSS	-	Space-Based Surveillance System
SEP	-	Solar Energetic Particle
SESAR	-	Single European Sky ATM Research
SEU	-	Single Event Upset
SIGINT	-	Signals Intelligence
SMOS	-	Soil Moisture Ocean Salinity

SOHO	-	Solar and Heliospheric Observatory
SoL	-	Safety of Life
SPOT	-	Satellite Pour l’Observation de la Terre
SSA	-	Space Situational Awareness
SSA-NEO	-	Near-Earth Object segment of the European Space Situational Awareness Programme
SSA-PP	-	Space Situational Awareness Preparatory Programme
SSA-SST	-	Space Surveillance and Tracking segment of the European Space Situational Awareness Programme
SSA-SWE	-	Space Weather Event segment of the European Space Situational Awareness Programme
SSL	-	Solid State Laser
SST	-	Space Surveillance and Tracking
SSTL	-	Surrey Satellites Technology Limited
STM	-	Space Traffic Management
SWE	-	Space Weather Event
SWPC	-	Space Weather Prediction Centre
TCBM	-	Transparency and Confidence-Building Measure
TEN-T	-	Trans-European Transport Network
TIRA	-	Tracking and Imaging Radar
TROPOMI	-	TROPOspheric Monitoring Instrument
TV	-	Television
UKSA	-	United Kingdom Space Agency
UNCOPUOS	-	United Nations Committee on the Peaceful Uses of Outer Space

UNIDIR	-	United Nations Institute for Disarmament Research
UNOOSA	-	United Nations Office for Outer Space Affairs
US	-	United States
USAAF	-	United States Air Force
USSSN	-	United States Space Surveillance Network
UV	-	Ultra-Violet
VHF	-	Very High Frequency
WAAS	-	Wide-Area Augmentation System

Acknowledgements

This Ph.D. project and thesis would not have been possible without the help and support of a number of friends and family members to whom I am eternally grateful. In particular I would like to thank my supervisors, Luis Lobo-Guerrero and Peter Adey, for their invaluable support and tireless enthusiasm for my project regardless of the time of day or their location across the globe, and my examiners John Vogler and Michael Sheehan. Many thanks also to the members of the Emerging Securities Unit at Keele – and in particular Barry Ryan, Chris Zebrowski, Corey Walker-Mortimer, Helen Parr and Rob Emerton – and to Claudia Aradau, Marieke de Goede, Marijn Hoijtink, Stephanie Simon and Ruth Fletcher, all of whom have offered invaluable advice on my project as it progressed and developed. Andy Hodder and Rebecca Spiteri have patiently supported me throughout the peaks and troughs of the project, providing encouragement and advice. Finally, I would like to say thank you to my brothers and my parents for forgiving my occasional outbursts of seemingly nonsensical thoughts, and especially to Laurence Slann for reading over my translations and Angela Slann for reading and commenting on endless drafts of my work without complaint.

1 Introduction

From the second half of 2012 and through to the end of 2014, the European Union (EU) Space Expo travelled around Europe, stopping in a number of countries, including Denmark, France, Finland, Belgium, Austria, Cyprus and the United Kingdom. At all of these venues, an inflatable bubble was erected containing a series of displays and holographic imagery, as well as a small stage for experts in European outer space activities to offer brief introductory talks on their area of expertise. The objective of the exhibition was to introduce visitors to the wide variety of applications that have been enhanced or made possible through the use of outer space technologies. The displays and talks focused upon three projects: Galileo, the European Geostationary Navigation Overlay Service (EGNOS) and Copernicus, formally known as Global Monitoring for Environment and Security (GMES). These three projects, only one of which – EGNOS – is fully operational at the time of writing, represent some of the main EU investments in outer space. Galileo and Copernicus in particular have been described as the ‘flagship’ European outer space programmes (see Giannopapa and Oren, 2011; Nardon and Venet, 2011), with EGNOS being included alongside the Galileo programme as part of the wider project to provide improved Global Navigation Satellite Service (GNSS) signals to Europe. The exhibition included a series of videos explaining how the services provided by EGNOS, Galileo and Copernicus are already improving the lives of those living in Europe, as well as looking to the future and portraying how lifestyles, transportation, safety and labour will be further assisted and enhanced. Although the exhibition was aimed at raising awareness of outer space technologies and their applications, there was an implied message that these technologies are integral to European societies. However, there was a noticeable absence of information on how these services are to be secured.

Modern societies are largely dependent upon outer space technologies and applications. From relatively mundane activities such as digital television, to the remarkable and yet necessary precision offered by the atomic clocks of Global Navigation Satellite Systems (GNSSs). Although landline telephones and the internet might not be dramatically affected, a hypothetical loss of all satellites would cripple many aspects of 21st century societies (Black, 2011), including air and sea travel and banking. Given the navigation and remote sensing services that Galileo and Copernicus are expected to provide, it can be presumed they will become important assets for Europe and the EU in the future, both on a practical level of service-provision but also on a political level, as evidence of European outer space industry and the EU's position as an independent actor in outer space affairs. As Pasco (2009) highlights succinctly, the problem is thus:

> [i]f Europe wants to remain an independent actor in the space arena, it will […] have to find ways to protect its civilian dual-use space programs without relying on military options that have never been attractive to its member states and that have been deliberately precluded at the community level (p. 12).

The need for ensuring the security of the EU's outer space assets, which are framed in this thesis as being parts of critical outer space infrastructures, follows a wider trend of portraying critical infrastructures as points of vulnerability for the security, safety and wellbeing of terrestrial states, societies and populations (see Clemente, 2013; Cohen, 2010;

Council of the European Union, 2008a; Egan, 2007 and US Department of Homeland Security, 2012).

This thesis focuses upon the space segments of European critical outer space infrastructures and their security. In doing so it poses four main questions:

1. Are outer space infrastructures critical infrastructures for the EU, and if so, why?
2. To what extent does the EU recognise this?
3. What risks and dangers does the EU perceive to be threatening to the space segments of European critical outer space infrastructures?
4. How is the EU attempting to ensure the security of the space segments of its critical outer space infrastructures against these risks and dangers, and how can this be conceptualised?

1.1 The issue at hand: (in)security in outer space

Although satellites have become established as an integral part of modern ways of life, they are vulnerable to a myriad of intentional and unintentional forms of interference. As will be discussed in more detail later, the EU and the European Space Agency (ESA) do not admit in public the risks or dangers from which they protect their outer space infrastructures, however the European Commission (EC) (2011a) has offered a general overview of the dangers it believes are posed to operations in outer space:

> [outer space] infrastructure is at risk of damage or destruction by natural phenomena, such as solar radiation and asteroids, and by other spacecraft and

> their debris. It is also under threat from electromagnetic interference, be it intentional or otherwise (p. 6).

This thesis divides forms of interference into two categories: intentional and unintentional, which are themselves comprised of a number of risks and dangers. Intentional interference to space segments generally comes in the use of anti-satellite (ASAT) weaponry or electromagnetic signal jamming to permanently or temporarily disable satellites, though interference with the operations of ground control infrastructures has the potential to be equally effective. Unintentional forms of interference, meanwhile, include space debris, solar flares, radiation and accidental signal interference from satellites sharing frequencies.

Intentional interference implies the use of force or technology by one party against the outer space assets or ground control segments of another party. While there has not yet been an instance of operational satellites being attacked by anti-satellite weaponry, the technology was developed by both the USA and the Soviet Union during the Cold War (Moltz, 2008; Vogler, 2000), although there was then a hiatus in testing until the Chinese and US ASAT events in 2007 and 2008 respectively (Moltz, 2008). The threat posed by the continued development of technologies capable of interfering with satellite operations has been recognised by numerous actors dependent on satellite applications, including the North Atlantic Treaty Organisation (NATO), which, in its 6th Strategic Concept, warned that:

> [a] number of significant technology-related trends – including the development of laser weapons, electronic warfare and technologies that impede access to space – appear poised to have major global effects that will

> impact on NATO military planning and operations (North Atlantic Treaty Organisation, 2010).

While ASAT technology itself has been proved successful through testing, there is the risk of significant space debris generation, a factor which contributed during the Cold War to the decision of US and Soviet leaders "to minimize risks by establishing norms of unacceptable space behavior" (Moltz, 2008: 65). Alongside the suspension of ASAT testing in the 1970s, such norms included the prohibition of nuclear testing in outer space, which had proved dangerous to satellites and astronauts thousands of miles away from the detonation. On 9th July 1962, as part of Project Fishbowl, the US detonated a 1.4 megaton hydrogen bomb, named Starfish Prime, at an altitude of 248 miles, which led to a significant increase in the number of electrons present within the Van Allen radiation belts surrounding the Earth (Moltz, 2008: 119). Furthermore, the electromagnetic pulse (EMP) discharge from the Starfish explosion eventually disabled six satellites: one British, one Soviet and four American (Hoerlin, 1976: 25-26). Although the US did not immediately cease its exo-atmospheric nuclear testing program, after the failure of the third attempted Bluegill test on 25th July 1962 and months of tense negotiations between the US, the UK and the Soviet Union, there was eventually an agreement between the three states to sign the Partial Test-Ban Treaty (PTBT) in Moscow in July 1963. As well as banning the testing of nuclear weapons in outer space, the treaty also prohibited testing in the Earth's atmosphere and under-water (Moltz, 2008: 139).[1]

While there are many forms of unintentional interference, two in particular – space debris and the accidental overlapping of frequencies – have been the subject of

---

[1] For a more detailed analysis of the negotiations and events which led up to the Partial Test-Ban Treaty, see Moltz (2008: 118-142)

international efforts to counter them. Space debris has been a growing issue since the early years of human space exploration. By the mid-1960s, the National Aeronautics and Space Administration (NASA) had begun considering the problem, a process which was placed on the international stage in the 1970s following a series of ASAT tests undertaken by the Soviet Union which further increased the amount of debris in orbit (Moltz, 2008: 126). Recently, international efforts have included mitigation guidelines proposed by the Inter-Agency Debris Coordination Committee (IADC) in 2003 and approved by the United Nations (UN) General Assembly in 2007, while the US in particular has been active in ensuring that companies and agencies launching satellites comply with stringent regulations.[2] With regards to frequency overlapping, the International Telecommunications Union (ITU) is responsible for overseeing the existing regime concerning frequencies by allocating them to states, which are then charged with regulating distribution and compliance with international norms and agreements.

1.2 Outer space and the astrophysical environment

While outer space is undisputedly a vast area, human activity is, with the exception of a small number of scientific probes, limited to a solar system which is a comparatively minuscule portion of the universe. Even then, the majority of this activity, including manned spaceflight, has thus far only extended to the Moon, Earth's celestial satellite. Therefore, terms such as outer space security are intrinsically linked to the technological capabilities of the human race; we, as humans, rarely consider future security issues and applications of satellites and spacecraft travelling regularly beyond the Moon. Dolman (2002), for example, admits that what he terms 'Solar space', in other words everything in

---

[2] These regulations include the 1995 *NASA Safety Standard*, the 2007 *Process for Limiting Orbital Debris* again published by NASA (National Aeronautics and Space Administration, 1995; 2009) and the 1997 *Orbital Debris Mitigation Standard Practices* published by the US government (United States Government, 1997).

our solar system beyond the gravity well of the Moon, is of less importance than the space between the surface of the Earth and the Moon, as “exploration into this region using current technologies will be quite limited” (p. 70). Dolman does however note that “the exploration of solar space is the next major goal for manned missions and eventual permanent human colonization” (p. 70), implying that the limits of policy formulation and academic thinking will steadily expand alongside advancing technologies.

1.2.1 Delimiting the separation between the Earth’s atmosphere and outer space

When discussing human activities in outer space, a first question to consider is where the Earth’s atmosphere ends and outer space begins. While technological and financial restrictions mean that human activities do not regularly extend beyond 40,000km, it is important to identify the lower limit for operations that can be described as taking place in ‘outer space’. Although at first glance this question may well appear simple, there is anything but a consensus amongst policy-makers, lawyers and academics over the boundary between the atmosphere and outer space. The significance of this conceptual and legal impasse over should not be underestimated; as Oduntan (2012) notes:

> [t]he legal distinction between airspace and outer space and the two bodies of law governing them is ultimately very necessary for the smooth conduct of air and space activities. In spite of the acknowledged commercial, strategic, political and environmental importance of air and space activities, the province and exact scope of the applicable laws have not been determined (p. 282).

If nothing else, a distinct demarcation between airspace and outer space is required to denote where national sovereignty can be claimed and where it cannot (Banner; 2008; Harris and Harris, 2006; Oduntan, 2003; 2012). Additionally, it can be argued that any international legal agreements on activities in outer space are inherently limited if the domain to which they pertain is not clearly defined. Within the context of this thesis, the demarcation of airspace/outer space is necessary to differentiate between activities that are normalised in one domain yet remain issues of concern in the other. The testing of weapons systems, discussed further in chapter 4, is a pertinent example; it is common practice for states to test the capability of their weapons systems to destroy targets located within the confines of the Earth’s atmosphere. In contrast, the testing of extra-terrestrial weapons is a controversial practice, with recent ASAT testing by China and the US resulting in vocalised objections from spacefaring states. Moreover, delimiting between airspace and outer space clarifies the scope of this thesis, which focuses on the security of the space segments of outer space infrastructures.

A popular demarcation between airspace and outer space is the Kármán line, proposed by the Hungarian-American aerospace engineer Theodore von Kármán, which establishes that outer space begins at an altitude of 100 km, where space operations first become practical (Ministry of Defence, 2012: 1-2). Although the Kármán line has been adopted by some international institutions, such as the Fédération Aéronautique Internationale (FAI), there have been objections: for instance, Rendleman (2010) notes that the US is reluctant to formally acknowledge it, as doing so may allow states to oppose the over-flight of space objects after they re-enter the Earth's atmosphere (pp. 16-17). The permanence of the Kármán line has also been called into question by Oduntan (2003), who argues that “the desirable legal demarcation regime should ideally be of a near permanent if not final nature and not based upon the possibility of change due to slight changes in technological progress” (p. 74).

Despite the continued legal debates surrounding it, for the purpose of this thesis, the Kármán line will be employed to demarcate the boundary between airspace and outer space.[3] The reason for this being that it is grounded in the limitations of aerodynamic lift and even though some aircraft under development may be able to exceed that altitude (Oduntan, 2012: 299), at the time of writing the vast majority cannot. The intention here is not to argue in favour of the adoption of the Kármán line in international law, but rather only to provide a distinction between airspace and outer space in the context of this thesis.

1.2.2 The orbital regions of near-Earth space

Human activities in outer space, as mentioned above, are largely restricted to the space between the Earth and the Moon. Specifically, many of these activities take place at different altitudes above the Earth, which are commonly classified into four different geocentric orbital regions: Lower Earth Orbit (LEO), Middle Earth Orbit (MEO), High Earth Orbit (HEO) and Geosynchronous Orbit (GEO).[4] A brief summary to these regions is provided to offer the reader an introduction to the astrography of near-Earth space and the variety of orbits populated by satellites. The requirements of satellite operations often necessitate the use of specific orbital altitudes and inclinations, however as some risks and dangers are more common in certain altitudinal regions, satellite security must be adapted as necessary. It is therefore important to highlight the division of near-Earth space into the orbital regions listed above to provide context for later discussions concerning altitudinal-specific risks and dangers.

---

[3] For summaries of the historical and legal debates surrounding the delimitation of airspace and outer space, see Banner (2008) and Oduntan (2003; 2012).

[4] See figure 1.1 for a diagram of these orbital regions of near-Earth space.

Lower Earth Orbit extends from 150km to 2000km (Inter-Agency Space Debris Coordination Committee, 2007: 6) and is one of the most densely populated areas of near-Earth space. Because of its close proximity to the Earth, many imaging satellites use this orbit, as do manned spacecraft such as the International Space Station (ISS) (Johnson-Freese, 2009: 69). Indeed, the number of satellites and operations taking place in LEO has led MacDonald (2007) to note that “space – and in particular the Lower Earth Orbit […] – can no longer be considered remote. The journey through the Earth’s atmosphere is now made on an almost weekly basis” (p. 594).

Above LEO, Middle Earth Orbit ranges from 800km to 35,000km and is home to GNSSs such as the NAVSTAR Global Positioning System (GPS) (Dolman, 2002: 65-66) and the European Galileo programme (European Space Agency, 2007). However, MEO is a hostile environment as it includes both the Van Allen radiation belts, which necessitate protection against the harsh conditions (Johnson-Freese, 2009: 69; Royal Academy of Engineering, 2013: 12).

Extending beyond 35,000km is the region known as High Earth Orbit. This region offers the best coverage of the Earth with the minimum number of satellites and includes Geosynchronous Orbit (Dolman, 2002: 66). GEO has an altitude of approximately 35,800km (Johnson-Freese, 2009: 69), which allows for an orbital period – the time it takes for a satellite to revolve around the earth – of exactly one day. Satellites in GEO with an inclination of 0º are known as being in Geostationary Orbit (GSO), as they remain in a fixed relative position above the equator. Satellites in GSO can ‘see’ 28 per cent of the Earth’s surface, while their ‘stationary’ position offers continuous contact with antennae on Earth. Consequently, GSO is populated largely by communications and weather satellites (Dolman, 2002: 66), leading Collis (2009) to contend that it is “Space’s [*sic*] most valuable position” (p. 47). Highly elliptical orbits are also classified as being located mainly in HEO and are characterised by having apogees higher than GEO (Topychkanov, 2010). An example of such a highly elliptical orbit, Molniya orbits have an apogee up to 40,000km in altitude enabling a wide coverage of the Earth’s surface and an orbital period of roughly half a day (see figure 1.2). Although not as much energy is required to launch satellites into a Molniya orbit, reducing costs, the nature of the orbit means that those satellites will pass through the Van Allen belts four times per day, increasing their exposure to energetic charged particle radiation.

Just as this thesis requires a demarcation between airspace and outer space, it is worthwhile defining what is considered to be 'near-Earth space'. Although attempts to divide outer space into a series of neat regions must be met with some trepidation, not least for the risk of falling into the classical astropolitical arguments of Dolman (2002), the imposition of some astrographical limits is required. In this case, near-Earth space is considered to be the expanse of outer space most used by human outer space activities; in other words the area beginning at the Kármán line and extending to the furthest Molniya elliptical orbit (40,000km).

The demarcations of the minimum and maximum altitudes of near-Earth space used in this thesis are based on current aeronautical and technological capabilities; it is admittedly a technoastropolitical delimitation of the astrographical region referred to as ‘near-Earth space’. Those demarcations are therefore applicable only in the context of this thesis and the limitations regarding orbital operations which exist at the time of writing. Should sub-orbital flight become common above the Kármán line, then in all likelihood that boundary between airspace and outer space will have to be reconsidered. Equally, the region considered to be near-Earth space may well have to be enlarged if and when human outer space activities regularly extend beyond Molniya orbits.

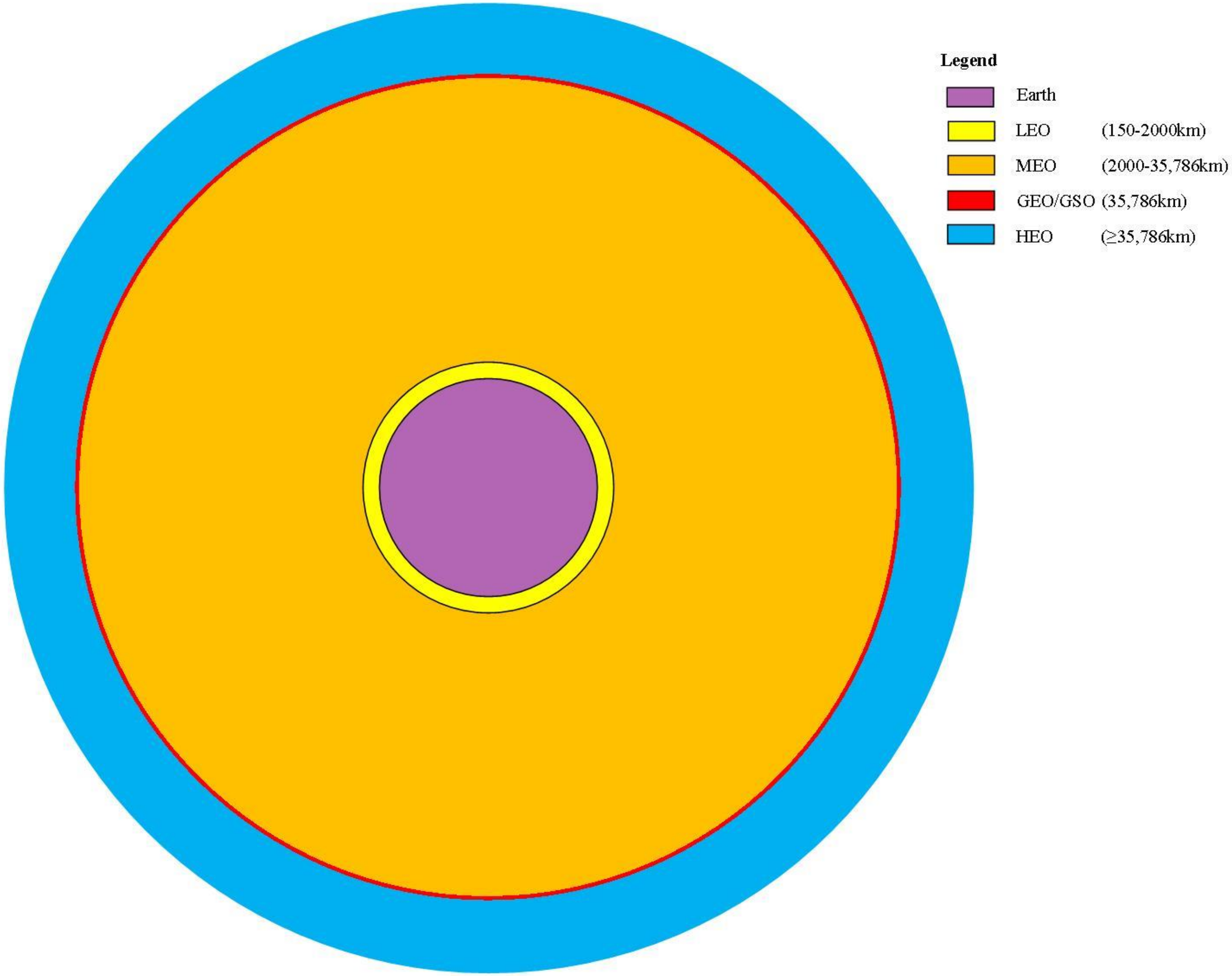

Figure 1.1: The orbital regions of near-Earth space (to scale 1:300,000,000)

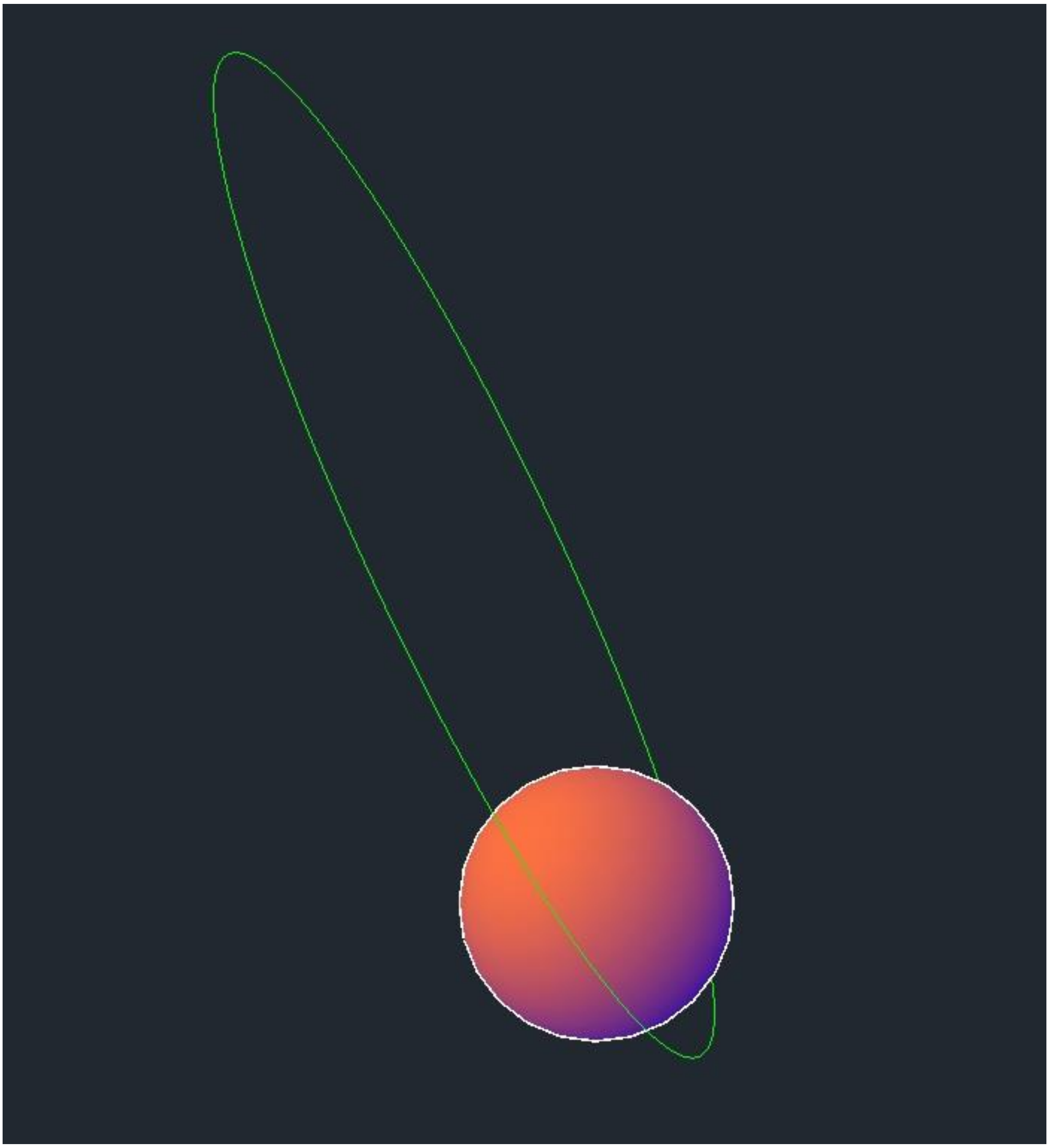

Figure 1.2 Illustration of a highly elliptical orbit

1.3 The foundations and context(s) of critical astropolitics

Rather than try to summarise the entirety of the astropolitical literature concerned with outer space affairs, which would be an almost impossible task, there follows a brief review of the arguments and theories of authors who take different approaches to the subject. Human activity in outer space, albeit largely undertaken by satellites under the command of humans on Earth, has produced outer space in a form which reflects the current requirements and expectations of the domain. Sheehan (2007) contends that:

> although we as humans live in a physical universe, much of the 'world' we inhabit is intersubjectively constructed through our mutual understandings of what constitutes reality. We act in terms of our beliefs, values, theories and understandings of the 'reality' we perceive […] We perceive outer space in a particular way, as a particular kind of realm, in which certain types of activity are possible, even expected, while others are frowned upon or specifically forbidden (p. 5).

This is illustrated perfectly, though perhaps unintentionally, by Caldicott and Eisendrath (2007), who name the first chapter of their book 'A brief history of outer space', even though it begins in 1958 with the launching of Sputnik 1. It is almost an insinuation that outer space did not exist prior to human expansion into the domain and that, for all intent and purpose, 'history' began with Sputnik. Whilst obviously inaccurate, there is nevertheless some truth in so far that outer space, as we conceive it today, did not exist prior to Sputnik. The launch of the first man-made satellite into a stable orbit transformed outer space into a domain of possibilities for supporting terrestrial systems and societies. Outer space has subsequently become a crucial support mechanism for terrestrial modes of life through the activities taking place there, and consequently space policies, programmes and laws are all directed towards maintaining this assistance.

There are two categories through which outer space is produced. The first is imaginations of outer space; how policy-makers, lawyers and non-experts conceive and understand outer space. These imaginations are internally reproductive, in that they reflect the conceptions of outer space yet simultaneously influence those conceptions. The second category is the use of outer space; how space programmes and the services provided by satellite networks produce outer space based upon terrestrial needs. In addition, both aforementioned categories are mutually constitutive; the imaginations of outer space shape the visions upon which space programmes are developed, while the achievements and realities of the space programmes serve to inspire and foster new imaginations.

A detailed account of how outer space has been imagined, and arguably constructed, in the years since the launch of Sputnik is beyond the intentions of this chapter.[5] Rather, it will attempt to illustrate how outer space is conceptualised in the current (astro-)political climate by reviewing existing literature and scholarship in the fields of critical geopolitics and astropolitics.

1.3.1 Astrographical and astropolitical imaginations of outer space

At face value, astrography is very similar to geography, in that while the latter applies to the earth (*geo*), the former relates to outer space (*astro*). However the phenomena being studied are naturally quite different: whilst geography is split between human and physical disciplines, the limits of astrography have yet to be specifically determined, thus numerous areas of interest could potentially fall within its mandate. This is not necessarily a drastic flaw though; in its current form, astrography offers the opportunity and framework for a broad study of the spatial and exploitative characteristics of outer space. However, MacDonald (2007) warns that "[w]e must be alert to the 'declarative' ('this is how the Outer Earth is') and 'imperative' ('this is what we must do') modes of narration that astropolitics has borrowed from its terrestrial antecedent" (p. 609).

---

[5] For a thorough account of how conceptualisations of the domain of outer space have developed since 1957, see Sheehan (2007).

Additionally, the advantages and limitations of geography equally apply to astrography: to paraphrase Ó Tuathail (1996: 2), 'astrography is not something already possessed by outer space but an active writing of outer space by an expanding, centralising imperial state. It is not a noun, but a verb, an *astro-graphing*, outer space-writing by ambitious endocolonising and exocolonising states who seek to seize space and organise it to fit their cultural visions and material interests'.

An example of this is the astrocartographical practice of mapping/tracking satellites' orbits around the earth; they are supposedly revealing the hidden vertical element of contemporary life but arguably serve only to obfuscate further. Astrographical maps/tracks reveal the positions of some satellites or orbits, but only those which the owners (state or otherwise) are willing to reveal, and even then, the user is allowed to choose which satellites' orbits they wish to see, enabling an orderly perspective. However, orbital tracks are projected upon a map of the Earth, showing users where, compared to their terrestrial position, satellites are passing overhead. This though leads to an obfuscation of the astrographical 'reality' of outer space, where so-called 'near-Earth' space is crowded by satellites on their own orbital paths. Furthermore, the orbital tracks do not display the vertical orbit of satellites, only their projected geographical paths, thus ignoring a vital spatial element of satellites' orbits, and there is little or no display of deviation from predicted orbital paths. The mere existence of orbital tracking is arguably problematic, as it emphasises the human exploitation of outer space, ignoring areas or orbits which are not used by humans and their material assets.

The obfuscations created by orbital tracking are arguably founded upon perceived geographical and astrographical permanence. Orbital tracking software project predictions of 'live' events (orbiting satellites) upon a static cartographical representation of the Earth. This juxtaposition of highly mobile (albeit unidirectional) satellites upon a static Earth serves only to reinforce a number of geopolitical and cartographical fallacies. The specific cartographical representation of the Earth differs depending upon which orbital tracking software or website is used, however state boundaries are generally included as a means of illustrating over which states a particular satellite is travelling at a moment in time. However, providing states as the cartographical reference for satellites' travels only reinforces the perception of the state being the "fundamental unit of society" (P. Steinberg, 2012).

The division of near-Earth space into Lower Earth Orbit (LEO), Middle Earth Orbit (MEO), Higher Earth Orbit (HEO), Geostationary Orbit (GSO), Geosynchronous Orbit (GEO) and Polar Elliptical Orbit (PEO) arguably highlights yet another astrographical limitation: while they represent astrophysical and gravitational conditions which enable satellite operations around the Earth, the division of near-Earth space into such regions emphasises the man-made presence in outer space. In other words, near-Earth space is mapped based upon its technological exploitation by humankind, with the Earth as a societal, as well as astrophysical, referent.

The emergence of astropolitics has occurred in a similar fashion to astrography, with its proponents taking an approach associated with terrestrial politics – in this case geopolitics – and applying it to the extra-terrestrial dimension. It therefore, like the case of astrography discussed above, comes with the advantages and disadvantages of geopolitics. However, before astropolitics can be discussed in any detail geopolitics, and critiques of it, must first be reviewed.

1.3.2 From geopolitics to critical geopolitics

Geopolitics as a discipline has its origins in the late 19th Century, with years of European imperial ambitions and campaigns culminating in a situation whereby European world maps became “for the first time relatively occupied” (Ó Tuathail, 1996: 25; see Sparke, 2007: 339). Geopolitics has been heavily associated with the *Geopolitik* of Nazi Germany in the 1930s, to the extent that French accounts of geopolitics still struggle to broach the subject and its history (Retaillé, 2001: 35), though there is perhaps a certain irony that the French academic distaste for the study of geopolitics is itself borne of an historical geopolitical rivalry. Despite the assertions of Raffestin (2001: 10), the ‘classical’ geopolitical approach developed from scholars in the late 19th and early to mid-20th Centuries who were “fundamentally concerned with the role that *inter alia* location and resources play in the exercise of power over territory” (Dodds, 2010a); these scholars generally held a common understanding of permanence in geography, a perception which Ó Tuathail (1996) terms the ‘geopolitical gaze’. However, geography – either human or physical – is not permanent; it fluctuates thanks a multitude of factors, including societal changes, migration, continental drift and erosion but to name a few. Ó Tuathail (1996) argues that rather than emphasising its constituent elements, classical geopolitics (and geo-power in general):

> depends on a *suppression* of geography and politics. In its spatializations, biologization, linnaeanization, strategization, and naturalization of the historical, it works to degeographicalize and depoliticize the study of international politics (p. 53).

Additionally, while geopolitics purports to address global issues, in reality “it has instead offered a means of affixing and calibrating the meaning of the local within the global whole” (Ó Tuathail, 2010: 256). Geopolitics and geoeconomics – the former’s supposed post-Cold War replacement – are, as Sparke (2007) puts it, “better understood as geostrategic *discourses*" (p. 340, original emphasis), a focus which pervades much of the scholarship on critical geopolitics (Müller, 2010; Ó Tuathail, 2002). In particular, Ó Tuathail and Dalby (1998a) argue that the geopolitics of the Cold War era was no more than a "powerful and pervasive political ideology that lasted for forty years" (p. 1). In this way, the political foundations of geopolitics belie its attempts to reveal the 'truth' behind the relationships between geography and foreign policy formulation. It is, in the words of Ó Tuathail (1998), no more than "a particular mode of representing global space" (p. 22).

Ó Tuathail (1994; 1996) takes a Derridean deconstructive approach to critical geopolitics, attempting to deconstruct geopolitics by focusing upon the contexts in which geopolitics and geopolitical writings emerge. He uses hyphens to divide words "so the unseen conceptual marks that have so delimited our existing understandings of maps, geography and geopolitics can be rendered visible" (1994: 526). Consequently, geopolitics becomes *geo-politics* and geography becomes *geo-graph-y*,[6] while the term *geo-power* plays an important role in emphasising Foucauldian power/knowledge relationships. This is exemplary of the wider critical geopolitical approach; with close attention being paid to what is revealed and hidden by geopolitical discourses. In this light, geo-politics – "the politics of writing global space" (1996: 18) – is not separate to geopolitics, it is a problematic of the latter:

> Geo-politics does not mark a fixed presence but an unstable and indeterminate problematic; it is not an 'is' but a question. The hyphen ruptures the givenness of geopolitics and opens up the seal of bonding of the 'geo' and the 'politics' to critical thought. In undoing the symbolic functioning of the sign, its

---

[6] Ó Tuathail's geo-graph-y pertains, in his words, to "an open-ended inscribing, delimiting, and engraving of the earth/globe/world. To study geo-graph-y, then, is to study the projection of geo-graphs striving for signification; it is to study the graphing/weaving/writing of a geo/world/system" (1994: 530).

> semantic instability, ambiguity, and indeterminancy are released. The sign lies open before us, a disrupted unity in question, a sign of a textual weave involving geography and politics (1996: 67).

Ó Tuathail does not aim to provide a comprehensive theory; he contends that critical geopolitics works to reveal the problematic(s) of geopolitics, rather than offer an alternative (1994: 527). This is not to say that fieldwork and original research is discouraged, far from it; he recommends that “critical geopolitics can deepen its critical practice by grounding itself in regional research” (2010: 257). However the emphasis remains on the revealing of hidden discourses within geopolitical scholarship. In this light, he argues that geopolitics is yet another form of ‘geo-power’ that is:

> a convenient fiction, an imperfect name for a set of practices within the civil societies of the Great Powers that sought to explain the meaning of the new global conditions of space, power, and technology. It names not a singularity but a multiplicity, an ensemble of heterogeneous intellectual efforts to think through the geographical dimensions and implications of the transformative effects of changing technologies of transportation, communications, and warfare on the accumulation of exercise of power in the new world order of ‘closed space’ (1996: 15).

The Eurocentric nature of geopolitics permeates Ó Tuathail’s work and contributes the wider argument that the geopolitical culture assists and enables imperialism (Dalby, 2008; Ó Tuathail, 1996). Indeed, he contends that “[g]eopolitics is state philosophy, a technology of govern-mentality. It was conceived and nurtured in the imperial capitals of the Great

Powers, in their learned academics, in the map and war rooms of ambitious expansionist states" (p. 1998: 23). It also leads to a state of affairs identified by Agnew (1994), whereby the notion of the territorial state is immortalised in classical geopolitical literatures, as well as many international relations studies, although Ó Tuathail's (1998) arguments imply a mutually dependent relationship whereby the state relies upon geopolitical imaginations for justification of its existence and vice versa. The proliferation of the state as the common form of political organisation owes much to European colonialism and imperialism, to the extent that Agnew contends that "the territorial state as a primary mode of political organization is no older than the 18th century" (p. 65). Importantly, Agnew is not suggesting that territory itself is a problem, rather that the ways in which it is conceived are problematic (Agnew, 2010: 779; Elden, 2010: 757). The relevance of this scholarly incongruity to geopolitics is the context in which many classical geopoliticians were writing; their Eurocentric perspective meant that their concerns were with the continued existence of the state as a model of political organisation, rather than analysing its historical emergence (Ó Tuathail, 1996).

Although critical geopolitics emerged at the end of the Cold War and its proponents were primarily concerned with interrogating and critiquing the spatial and political foundations upon which states' foreign policies were formed, its relevance has by no means diminished (Dalby, 2008; 2010; Ó Tuathail, 2010). Empires and imperialism are returning to – if they had ever truly left – geopolitical scholarship (see Parker, 2010), while "much blood and treasure is still involved in military conflict, and many wars are justified in language structured in explicitly geographical terms" (Dalby, 2008: 415). Sparke (2007) notes that the fetishisation of space and place remains an integral aspect of contemporary US foreign policy-formulation; he argues that the use of terms such as 'axis of evil', 'failed states' and 'rogue regimes' creates a "geopolitical script of fear" (p. 340). This geopolitical language also creates a geographical and moral divide between ‘good’ and ‘evil’, as seen in the justifications for instigating conflict with Iraq in 2003 (Sparke, 2007). Geopolitics, then, is far from obsolete, and consequently critical geopolitics, in its desire to interrogate the foundations and assumptions of geopolitics, remains equally pertinent. This scholarly relationship extends beyond the atmospheric confines of the Earth: as a projection of geopolitics upon outer space, classical astropolitics – and Astropolitik in particular – is another example of the need for critical interrogation into the tacit spatialisation of statehood and foreign policy-formulation.

1.3.3 The context(s) of contemporary astropolitics

It is extremely difficult, if not impossible, to think and write about human exploration and exploitation of outer space without spatialising the issues at hand. Outer space, whilst a vacuum, is a spatial domain and the variables of distance, location and time exist largely as they do on Earth. It could therefore be argued that anyone writing about outer space affairs from an international relations perspective is in some way astropolitical, or at the very least touches upon astropolitical issues. On the other hand, if astropolitics is taken to be an extra-terrestrial projection of geopolitics – a point of view taken by Havercroft and Duvall (2012) – then close attention must be paid to the context in which astropolitical arguments and writings are made in order to fully understand them. In the same way that Ó Tuathail (1996) contends that “[g]eopolitics is not a concept that is immanently meaningful and fully present to itself but a discursive ‘event’ that poses questions to us whenever it is evoked and rhetorically deployed” (p. 17), the contexts in which astropolitics is employed in scholarly writing are themselves revealing.

Astropolitics emerged as an academic concept after the end of the Cold War, when near-Earth space was becoming increasingly inhabited by satellites from a multitude of states, rather than just the US and the USSR. Near-Earth space was no longer a domain to be explored; it was a domain to be exploited. Astropolitics is, in effect, the projection of geopolitics upon the domain of outer space (Havercroft and Duvall, 2012: 43); indeed, one of the main proponents of the approach, Everett Dolman (2002), unashamedly bases his Astropolitik upon the writings of Mahan and Mackinder. Wang (2009) should also be included in the list of astropoliticians, as he overtly states his interest in the approach in the title of his article. However, despite presenting them as background to his arguments, he fails to adequately engage with geopolitical or critical geopolitical literatures, taking astropolitics to be a direct projection of geopolitics into outer space with little regard for astrophysical and gravitational phenomena. Taking a wide perspective, whilst geopoliticians, particularly those of the late 19th and early 20th centuries, are keen on exploring the new spatial opportunities and problems offered by developments in transportation, communications and warfare (Ó Tuathail, 1996), astropoliticians explore similar opportunities and problems, only their focus is on outer space rather than the familiar land and seas of the Earth. While the issues at hand may vary wildly between the two disciplines, the conclusions are often quite similar.

1.3.3.1 Astropolitics and space power

When considering astropolitics, perhaps one most significant works thus far is Dolman's (2002) *Astropolitik Classical Geopolitics in the Space Age*, a monograph referenced in much of the astropolitical literature. When considering his theory of Astropolitik and, in particular the advocacy of space control, his classical geopolitical roots become prominent. Although, admittedly, the impermanence of geography does not apply as much to outer space[7] the context and underlying culture of his arguments are worthy of interrogation.

Dolman (2002) was one of the first scholars to introduce a notion of ‘astropolitics’, which he defined as “the study of the relationship outer space terrain and technology and the development of political and military policy and strategy” (p. 15). Dolman’s own approach to astropolitics, which he names ‘Astropolitik’, is developed from the classical geopolitics of Mahan and Mackinder and is, for the most part, concerned with the use of outer space to serve the terrestrial intentions of the US. Indeed, Dolman sees outer space as a domain to be strategically exploited through space control and the seizure of key choke-points, reflecting Astropolitik’s terrestrial origins and perhaps going some way to explaining his reverting to terrestrial strategic vocabulary when referring to the “terrain” (p. 15) of outer space. It could be argued though that by relying on the classical geopolitical writings of Mahan and Mackinder, Dolman’s Astropolitik is creating an intrinsic link between human activities on the Earth and those in near-Earth space. In other words, while the physical limitations and characteristics of near-Earth space may differ to those on Earth, the tactics and strategies that Dolman advocates for near-Earth space are very close, if not identical, to those employed on Earth. This is problematic, as while Dolman emphasises the importance of terrestrial geopolitical concepts such as choke-points and the heartland as integral to Astropolitik, the inherent vulnerability of orbiting satellites to both man-made dangers and natural phenomena means that the classical geopolitical thinking upon which Astropolitik is based is being adapted to an environment for which it was not designed. Admittedly, space control may well be possible for a state

---

[7] Ó Tuathail (1996) uses mountains, held by Spykman as an example of geographical permanence when in reality they exemplify the fluidity of the Earth’s geology, to critique the views of classical geopolitical scholars (p. 51). By and large though, astrophysical change occurs at such a slow rate that for the sake of human exploration and exploitation in the domain, astrophysical phenomena such as the Lagrange Points could arguably be considered permanent.

with similar material and financial wealth as the US, however the concept revolves around Earth-to-space and space-to-space weapons systems. The negation of these systems – possible through a myriad of ways from the destruction of the systems themselves or their ground control elements, or the interruption of signals from the ground control elements to the satellites – would seriously impact, if not end, an attempt at space control. This level of vulnerability implies a similar weakness to the one identified by Deudney (1985) when critiquing Reagan's proposed space-based Anti-Ballistic Missile (ABM) system, as:

> [i]n order to be effective, such a system would have to maintain continuous control not simply over North America but over the entire planet […] Thus the United States can only hope to regain its insular security by seizing the entirety of near space, which would fundamentally jeopardize the sovereign security of every other nation on the planet (p. 272).

Without moving too far into the hypothetical musings, it does not require a huge leap of the imagination to argue that many, if not all, other state and non-state entities – such as international companies and organisations with a vested interested in access to outer space – might in all likelihood react negatively to any definitive attempts at space control.

Dolman (2002) divides the space around the Earth into four regions based upon Mackinder's Heartland theory (p. 68): *Terra* or the Earth, *Terran* or Earth space, *Lunar* or Moon space, and *Solar* space (Dolman, 2002: 69-70). The first region, *Terra* or the Earth, represents the area "including the atmosphere stretching from the surface to just below the lowest altitude capable of supporting unpowered orbit" (p. 69). The second region, *Terran* or Earth Space, extends "from the lowest viable orbit to just beyond geostationary altitude (about 36,000km)" (p. 69), while the third region, *Lunar* or Moon Space, represents "the region just beyond geostationary orbit to just beyond lunar orbit" (p. 70). Finally, the fourth region, undoubtedly the largest, is Solar Space, which "consists of everything in the solar system (that is, within the gravity well of the Sun) beyond the orbit of the Moon" (p. 70). This last region highlights the Earth-centric technological basis for Dolman's division of outer space, as he chooses to group everything beyond the reach of contemporary human spaceflight together, "as expansion into this region using current technologies will be quite limited" (p. 70). It could be argued that this gives the strategic side of Astropolitik a fairly short lifespan, as it will need to be consistently reconfigured the moment that human spaceflight extends beyond its technological limits.

Dolman's four regions of space are not purely cosmetic; he bases many of his arguments on space control on these regions, and Earth space in particular, which he describes as, "like eastern Europe in Mackinder's design […] the most critical arena for astropolitics" (p. 70). Consequently, there appears to be within Astropolitik an inherent, if not necessary, compartmentalisation of outer space, which acts as an enabler for the aggressive strategies that Dolman advocates. This compartmentalisation is partially due to geopolitical foundations of Astropolitik, as even when referring to the vacuum of outer space, Dolman (2002) sees in gravitational phenomena and human technological capabilities a chance to apply classical Mackinderian (p. 40) and Mahanian (p. 38) geopolitical theories. Nevertheless, the compartmentalisation reveals the cultural foundations upon which Astropolitik is based; by establishing borders between areas in outer space, Dolman creates the possibility for them to be 'controlled'. He provides a spatio-temporal location for the normalisation of particular actions: Earth Space is where much of the current human extra-terrestrial exploration and exploitation takes place, whilst Solar Space is currently beyond the technological reach for all but scientific exploration.

Consequently, attempts at space control in Solar Space make little sense, yet they are to be expected within Earth space.

Dolman's Astropolitik can be closely associated with the concept of space power, a notion which has emerged in the early 21st century and is tentatively defined by Lutes *et al.* (2011b) as "the ability to use space to influence others, events, or the environment to achieve one's purposes or goals" (p. xiv). The concept is relatively broad, as "[i]t is not a single property, but a combination of factors. Space power is composed of a set of interrelated elements. It is not simply satellites and launchers. It is anything and everything a country can achieve through space" (Peter, 2010: 351). This said, there is no agreed definition of space power and significant divisions remain as to the conceptual limitations of the theory. For instance, Sheldon and Gray (2011) openly admit that their understanding of strategy, and consequently space power, is "unashamedly Clausewitzian" (p. 1), hence their definition of strategy as "the use that is made of force and the threat of force for the ends of policy" (pp. 1-2). The result is an approach to space power focused largely on military matters. Peter (2010), on the other hand, proposes that space power be defined as the

> total strength and ability of a State to conduct and influence activities to, in, through and from space to achieve its goals and objectives (security and military, economic and political) to affect desired outcomes in the presence of other actors in the world stage and if necessary to change the behaviour of others by exploiting the space systems and associated ground-infrastructure as well as political leverage it has garnered (p. 351).

Whilst military affairs and opportunities remain prominent in Peter's definition, it is nonetheless broader than the approach taken by Sheldon and Gray (2011), whilst being more detailed than the definition offered by Lutes *et al*. (2011b: xiv). Moreover, Peter (2010) goes on to contend that space power affects four areas of 'national' power; political, economic, military and cultural (pp. 351-352).

In addition to the lack of consensus regarding the definition of space power, it has been argued that a comprehensive theory of 'spacepower' is yet to emerge (Lutes *et al*., 2011b; Peter, 2010), a situation that has been the "subject of speculation on numerous plausible and seemingly implausible factors" (Sheldon and Gray, 2011: 2). Sheldon and Gray (2011) contend that:

> [s]ome of these impediments are unintentional and random incidents, phenomena and events that are the stuff of everyday defense planning and strategic decisionmaking [*sic*]. Other impediments are more insidious, the product of institutional practices and failings, or flaws in military and strategic culture (p. 2).

As Sheldon and Gray note, the concept is relatively young in comparison with its ground and naval equivalents and consequently there is not a vast literature on the subject. Nonetheless, some important contributions can be identified. As already discussed, Dolman's (2002) work on Astropolitik – and in particular his advocacy of the doctrine of space control – is an oft-referenced example of space power theorising.

Arguably however, there are two commonalities between the various definitions of space power; firstly, they are all predicated on the ability of actors to project power into, across and from outer space. Consequently, space power can be considered intrinsically astro-/geographical and astro-/geopolitical. A pertinent example of this is Oberg's (1999) assertion that "[t]he free exercise of space operations requires a launch site with ample downrange safety zones […] and usually a far-flung string of communications sites. This favors geographically large nations or those with good diplomatic relations with potential host nations" (p. 47).

The second commonality between the understandings of space power is that there is an inherent terrestrial focus (Pfaltzgraff Jr., 2011), as indicated by the emphasis Peter (2010) places on how space power complements a state's "goals and objectives […] in the world stage" (p. 351). The ultimate objective of space power is to enhance and increase the power that actor(s) wield on Earth, be it associated with military and strategic matters (Dolman, 2002; Sheldon and Gray, 2011) or economic affairs (Hertzfeld, 2011; Fuller Jr. *et al.*, 2011). This arguably affects the way through which near-Earth space is imagined in space power literature, insofar as it is portrayed as intrinsic to terrestrial power and thus arguably part of a wider sphere of planetary action. Particularly by proponents of the 'ultimate high ground' notion, near-Earth space is imagined as an extension of terrestrial activities, thus extending the limits of 'planet Earth' to the extremities of near-Earth space, or the Terran region, as Dolman (2002: 69) describes it. Indeed, the term Terran space implies such an extension of the planetary sphere as this region is still considered part of the Earth. With respect to Europe and the EU, Pasco's (2011) article on European space power focuses largely on military programmes and the means through which outer space assets can complement the European Security and Defence Policy (ESDP). Notably, the cultural impact of space power discussed by Peter (2010) – whereby outer space assets and technologies are used to foster a common identity amongst citizens – is not included.

Despite the focus upon the terrestrial consequences of space power, issues surrounding outer space governance are not ignored; Dolman's (2002) Astropolitik is a pertinent example of how primacy in outer space affairs has been portrayed as vital to achieving terrestrial dominance (space power), whilst Hays (2011) assesses the importance of a legal regime concerned with outer space activities to US space power capabilities. Nonetheless, there appears to be a trend within the space power literature to prioritise the terrestrial consequences of space power, with issues concerning outer space governance being of secondary importance.

Space power is often a relatively narrow concept, discussed with reference to single actors, which are often states or inter-state institutions. Some space power advocates – Dolman (2002), Oberg (1999; 2003) and A. Steinberg (2012) being prime examples – are explicitly concerned with how outer space activities are vital to US interests alone, with other spacefaring actors rarely mentioned. Whilst Pasco (2011) and Peter (2010) do include the capabilities of individual states during their discussions of European space power, their emphasis remains state-centric; the complex underlying relationships between national and European space industries are largely ignored. This said, there are exceptions to this narrow, state-centric approach. For instance, Sadeh (2011) concludes following his analysis of the need for environmental factors to be incorporated into conceptions of space power; "[o]ne implication broadens the scope of spacepower from a focus solely on national concerns to include regional and global concerns" (p. 21). Hays (2011) takes a similar approach, arguing that it is "imperative that the United States and all spacefaring actors think more creatively about using spacepower to transcend traditional and emerging threats to our [humankind's] survival" (p. 13).

Space power then is oriented towards the use of outer space and assets located therein to project power, whilst, as outlined below, outer space security is concerned with the protection of those assets and the services they provide. In astrographical and geographical terms, space power portrays near-Earth space as an extension of terrestrial power relations; near-Earth space becomes incorporated within the terrestrial sphere of activity, so to speak. With reference to security, space power theorists have traditionally been advocates of space weaponisation as a means of establishing and maintaining space power. This advocacy stretches back to Oberg (1999) and Dolman (2002; 2010), though remains through the writings of Dolman and Cooper (2011), Klein (2012), Pavelec (2012) and A. Steinberg (2012). Support for the weaponisation of outer space does not extend to all space power theorists however; Hays (2011) argues the need for a comprehensive legal regime to "illuminate paths toward and develop incentives for creating a better future" (p. 13) for humankind, while Krepon *et al*. (2011) contend that "it is possible to craft a regime based on self-interest to avoid turning space into a shooting gallery" (p. 6).

1.3.3.2 Cooperative astropolitics

Other astropolitical approaches place more emphasis upon the governance of outer space activities, rather than the impact those activities may have upon terrestrial power relations. This is not to say that they ignore the terrestrial benefits of outer space exploration and exploitation but rather that such advantages are not necessarily the overarching focus of those works. In other words, there is an astrographical difference between space power literature and that concerned with astropolitical governance, with the former arguably portraying near-Earth space as an extension of terrestrial matters and the latter introducing a separation between terrestrial and extra-terrestrial affairs.

Deudney (1985) is identified by Havercroft and Duvall (2012) as being, alongside Dolman (2002), one of the main proponents of astropolitics. Writing towards the end of the Cold War, he proposes an approach to outer space activities predicated upon cooperative technological development, arguing that this "offers the opportunity to rechannel the momentum of the arms race and to create at least an experimental working peace system"

(p. 303). Deudney encourages the redirection of efforts being put into the space weapons and ASAT systems towards cooperation between the USA and the USSR, positing that in addition to ensuring security from man-made threats to outer space assets, there may be an accelerated development of scientific and exploitative technologies for both near-Earth and deep space.

Whilst approaching the issue from the angle of environmental threats to satellites, Moltz (2008) is also a proponent of cooperation in outer space affairs. He notes "that surprising levels of restraint emerged during the first fifty years of space activity, despite a global context of political and military hostility" (p. 41). Taking the example of nuclear testing, he argues that the US and USSR found exo-atmospheric nuclear detonations to be "fundamentally incompatible with the pursuit of other goals in space" (p. 46). His monograph is a historical analysis of how environmental factors grew in importance and have been gradually attributed priority in national and international outer space policy-making. Whilst detailing the numerous obstacles that have arisen – such as the Anti-Ballistic Missile (ABM) Treaty negotiations – Moltz theorises the history of outer space affairs through the lens of cooperative outer space security predicated upon environmental factors and military restraint. He focuses upon EMP radiation and space debris as dangers which can emerge through military activities in outer space to justify his stance promoting the continued absence of space weapons, conventional or otherwise. In particular, he argues that given the emergence of a Chinese ASAT programme and the apparent resumption of US research and development into similar projects, there is a "need for a renewed and expanded international dialogue about space security" (p. 329).

The calls for a cooperative approach to outer space security are also echoed by Johnson-Freese (2006; 2007; 2009) and Sheehan (2007), amongst others. Johnson-Freese's focus is directed largely at the US, looking to promote policies which have the potential to foster cooperation with other spacefaring actors. Indeed, at times her 2009 monograph reads like a set of policy recommendations for the incoming Obama administration, and she concludes it by arguing that "[i]t is no longer enough to try to control the security dilemma that exists and is growing in space; it must be actively scaled back and dealt with from an entirely different perspective, toward making incremental but effective changes" (p. 145). Sheehan (2007) meanwhile contends that outer space affairs have historically been characterised by a "lack of novelty […insofar as] they have precisely mirrored terrestrial preoccupations and approaches" (p. 183). Nonetheless, he argues that outer space:

> still remains a distinctive arena […], because however much human activities there tend to reflect terrestrial realities, it continues to encourage international actors to believe that it *ought* to be possible to do things differently, and better, beyond the security of our home planet (p. 183, original emphasis).

Whilst noting the close historical association between terrestrial and extra-terrestrial international relations, Sheehan (2007) looks to separate the two; outer space is portrayed as a domain ripe for cooperation and collaboration that might not take place in the context of terrestrial geopolitical sensibilities.

In terms of the legal regimes promoting inter-actor cooperation in outer space, academic scrutiny has focused upon a number of areas, including the character and effectiveness of those regimes (see Vogler, 2000) and their impact on conceptualisations of extra-terrestrial sovereignty (see Stuart, 2012). Recently, the potential introduction of Transparency and Confidence-Building Measures (TCBMs) has received attention (see Robinson, 2010; 2011c; 2012), as have initiatives to promote sustainability through regime-based governance (see Arévalo-Yepes *et al.*, 2010; Brachet, 2012; Grego and Wright, 2010; Henri and Nozdrin, 2012; Meek, 2012; Rathgeber *et al.*, 2009; Weeden and Chow, 2012; Von Prittwitz, 2011; Williamson, 2012).

The astropolitical literature advocating cooperative approaches to outer space affairs take a wider, globalised view of near-Earth space. They portray the domain as one of mutual vulnerability, where seemingly isolated activities can rapidly have a wide-ranging impact (see Johnson-Freese, 2007; Moltz, 2008: 46). Debris generated through the destruction of a space object is indiscriminate with regards to the ownership of satellites. As Johnson-Freese (2007) notes, "if a [US] space weapon were used in space, it would create a debris cloud most dangerous to other U.S. space assets. Consequently, the United States gains nothing by having space weapons and potentially loses the most by using them" (p. 134). The promotion of cooperation through regime-based governance as means to resolve disputes and encourage sustainability conceptualises near-Earth space as a commons, where actors maintain the right to equal access to the domain and resources are either available to all or managed under a common property resource approach (Vogler, 2000; Weeden and Chow, 2012). In astrographical and astropolitical terms, the advocacy of inter-actor cooperation, regardless of whether it is supported by legal regimes and TCBMs, involves a conceptualisation of near-Earth space as relatively distinct from terrestrial affairs. While the terrestrial impacts of outer space activities remain important, extra-terrestrial governance is depicted as largely divorced from the political power relations on Earth.

1.3.4 Astropolitical discourses: spatialising and militarising outer space

Awareness of the temporal and contextual specificity of current astropolitical discourse is of great importance. As mentioned at the beginning of this chapter, the decision by Caldicott and Eisendrath (2007) to summarise the history of outer space beginning with Sputnik characterises the continued astropolitical obsession not only with human exploration and exploitation in outer space but also how they relate back to events on Earth. For all theoretical discussions of space control and the inhabitation of outer space and/or celestial objects, the focus of current national space policies and astropolitical scholarship remain firmly Earth-centric. This is not surprising; indeed it would be far more concerning if the majority of scholarly work were to ignore the impact of outer space exploration and exploitation on terrestrial societies. However, there must be some consideration for outer space and events taking place purely within the domain itself. Space debris for example, is an ever-growing issue,[8] though efforts to counter its proliferation have not yet earned enough political backing for a feasible solution to be found, despite many years of academic research and development (see, for example, Anselmo and Pardini, 2008; Rex, 1998; Wiedemann *et al.*, 2004). Although it may appear cynical to suggest that a reason for the absence of firm political support is the lack, thus far, of any significant impact upon terrestrial modes of life, the occasional and short-lived flurry of vocalised concern every time the ISS is forced to move to avoid a piece of debris, or the break-up of a satellite in orbit generates a new debris-field, belies the permanency of the problem.

The Earth-centric nature of many contemporary astropolitical writings arguably suggests an inability to escape the geopolitical foundations upon which astropolitics lies. The recurrent desire amongst scholars to identify national space policies and technological developments as part of a causal chain of events with terrestrial consequences, highlighted most prominently by widespread fears that the weaponisation of outer space will result in global hegemony and the erosion of state sovereignty, is inadequate. A much more urgent

---

[8] The proliferation of space debris and evolving efforts to mitigate it will be discussed in detail in Chapter 5.

problem posed by the potential weaponisation of outer space is the generation of space debris from the testing or use of ASAT weapons against orbiting satellites. This is not to argue that terrestrial and extra-terrestrial events and policies are divorced from each other, far from it. Nor should this argument be seen as advocating a reduction in efforts to ban orbital ASAT weapons systems: the possibility of space weapons being launched into orbit in the future is a harrowing one which threatens many technologies and infrastructures upon which modern societies depend. However, there is little to be achieved by postulating wildly about the potential for space weapons to support a global hegemony, particularly when such a capability on the scale required will not be feasible, financially or practically, for decades at the very least (see Spacy II, 2003).

It could be argued that the significant difference between space power and other astropolitical musings is the extent to which the relationship with terrestrial affairs and politics is prioritised. Space power literature is mostly concerned with looking back towards the Earth: outer space is portrayed as a domain to be exploited to the benefit of terrestrial societies. The ‘power’ under discussion can be considered a hybrid of terrestrial and extra-terrestrial capabilities but the end product is judged on what impacts are made upon terrestrial affairs. If space power is considered to emphasise the terrestrial consequences of space power capabilities then other approaches, although by no means ignoring the terrestrial impact of outer space activities, arguably choose to prioritise matters pertaining to the extra-terrestrial domain.

As a qualifier though, there is a contextual divide between space power and other astropolitical literatures; much of the academic work on space power is concerned solely with the impacts upon terrestrial actors and societies because the emphasis of said work is on the output of outer space assets. Meanwhile, the literatures concerned with the governance of outer space activities and outer space security – that is to say the security of outer space assets and their associated infrastructures – do not tend to have such a terrestrial focus.

Contemporary astropolitical writings tend to portray outer space assets as individual material objects operating outside of the confines of the Earth's atmosphere. This is problematic when the security of those assets comes under the spotlight, as in practice those assets are part of wider infrastructures comprised of ground and space segments. Few scholarly works have approached the problem from this angle, Cooper (2003) being a notable exception. As will be discussed in chapter 3 of this thesis, spacefaring actors are acknowledging both the complex infrastructures associated with outer space and their criticality to terrestrial societies.

Space power will be explored in more detail in chapters 2 through 4 of this thesis, which discuss the use of outer space critical infrastructures to complement and support actors' terrestrial policies. Nonetheless, the focus of this project is upon the security of those infrastructures rather than the projections of power that they enable. Consequently, this thesis does not intend to contribute directly to the debates surrounding space power but rather looks to identify relationships between European space power projection and the use of outer space assets for terrestrial policy-multiplication.[9]

1.4 Defining outer space security

The nature of the outer space environment means that security within the domain is markedly different to that which takes place on Earth. With the exception of those in geostationary orbit; satellites and other functioning man-made space objects do not remain in a fixed position relative to their ground control segments or each other, introducing a

---

[9] For the purposes of this thesis, policy-multiplication refers to the use of external factors to enhance the effectiveness or efficiency of a given policy. See chapter 2 for further discussion of policy-multiplication.

mobility divorced from the largely static nature of terrestrial critical infrastructure hardware. Moreover, satellites' orbits are spread vertically over thousands of kilometres, although some altitudinal regions are more popular than others. The three dimensional spatio-temporal nature of outer space operations means that satellite security often involves orbital trajectory prediction in addition to assessment of the risk posed by a specific threat or danger. In other words, dangers must be assessed in terms of which satellites will be passing through the affected three dimensional region in order to gauge the extent to which they can be considered threatening. Consequently, as will be discussed further with reference to anticipatory security in chapter 3 of this thesis, in addition to historical experiences, calculations of risks to satellites are dependent upon data from Space Situational Awareness (SSA) programmes. The capacity to 'know' threats in outer space is thus limited by technological capabilities.[10]

From a fairly ambiguous notion, outer space security emerges as an overarching term for specific issues related to the conduct of human activities in outer space, which then, because of dependence upon space assets, have a significant impact upon terrestrial geopolitics and modes of life on Earth. For instance, Moltz (2008) takes a fairly binary view of outer space security. He considers a state to be secure when "it enjoys the ability to conduct its activities free from harm" (p. 11). This definition is in itself problematic as complete 'security' or protection against all conceivable threats is, for all intents and purposes, impossible (Aradau *et al.*, 2008: 148; Krepon *et al.*, 2011: 4; Pursiainen, 2009: 727). Nevertheless, following on from his definition of security, Moltz' understanding of outer space security is that is the "*ability to place and operate assets outside the Earth's atmosphere without external interference, damage, or destruction* (p. 11, original

---

[10] For instance, concerns have been raised over the ageing US Space Surveillance Network (USSSN) and its continued capability to deliver accurate orbital trajectory data (see European Commission, 2013a).

emphasis), an approach which, as he acknowledges, implies that "all actors have enjoyed a high level of space security for most of the space age, with very few exceptions" (p. 11). While the fairly absolute nature of this definition could be considered problematic for the reason described above, it is difficult to conceive of an alternative definition which provides a strong foundation for a subsequent theory of outer space security. Nonetheless, perhaps the main point to be made is the scope of the definition; which implies the importance of environmental factors through the broad reference to "*external interference, damage or destruction*" (Moltz, 2008: 11, original emphasis). While this definition understands outer space security to pertain only to the activities that occur against objects in outer space, rather than any subsequent terrestrial impact of those activities, it nevertheless succeeds in encompassing many of the potential aspects of the concept and implicitly acknowledges the military and non-military factors involved.

Unsurprisingly, alternative definitions of outer space security exist. Although there is not the space here to account for all of them, as an example, the Space Security Index, a cooperative annual publication detailing events and developments in extra-terrestrial security, defines outer space security as "the secure and sustainable access to, and use of, space and freedom from space-based threats" (Jaramillo, 2012: 7). The first aspect of note within the definition is the inclusion of sustainability, which implies a long-term approach to security by ensuring that current actions and decisions do not affect future access to outer space. In this light, it could be assumed that preventing the proliferation of ASAT technologies and mitigating the generation of space debris would be an integral aspect of sustainable space security. Another important, and intriguing, focus of the aforementioned definition is the explicit emphasis upon 'space-based threats'. This phrase is problematic in two manners: firstly, it implies a human-centric understanding of the term 'threat', in other words only man-made dangers, and even then only those which are intentional, are worthy of being ‘threats’ to space assets. Although Jaramillo does not specify the man-made and intentional nature of the threats, the argument can be made that if unintentional dangers or threats – such as accidental collisions or the generation of space debris – were to be considered under this definition, it is likely that space security would never be achieved as ‘freedom’ from such factors will, for the foreseeable future at least, remain an optimistic and unachievable ambition. Therefore, in order for ‘freedom’ to be possible only intentional man-made threats can be considered. Although this is possibly a cynical perspective, the eradication of all threats, even only those based in space, is highly unlikely, particularly so if space debris and space weather are included. Secondly, the definition ignores the possibility of terrestrial ASATs being used in anger against satellites. This lapse is particularly significant given that the last two ASAT events, the Chinese test against FY-1C and the US destruction of USA-193, involved Earth-based systems.

Jakhu and Singh (2009) propose a wider definition than that of the Space Security Index; the “secure and sustainable access to, and use of, outer space and freedom from any threats or unreasonable (unjustified) barriers to such access and use” (p. 76). While they maintain the importance of access to outer space and sustainability, matters which they consider to be “at the heart of any discussion that surrounds the issue of space security” (p. 76), any ground- or space-based threats are included. The addition of “or unreasonable (unjustified) barriers” (p. 76) also implies that jamming or other temporary interference fall within their definition of outer space security, whilst maintaining the possibility that interference may be justified under specific circumstances. However, as with the definition of the Space Security Index, the emphasis on “freedom from any threats” (Jakhu and Singh, 2009: 76) is arguably unattainable so long as such threats exist *in potentia*, such as in the form of stockpiled ASAT weapons or the existence of space debris and technologies capable of intentional interference.

Given the inclusion of both ground- and space-based threats within Jakhu and Singh's definition, it is being broadly adopted for the purposes of this thesis. However, bearing in mind the aforementioned unattainable nature of the condition of 'freedom' from such threats present in the definitions of both the Space Security Index (Jaramillo, 2012) and Jakhu and Singh (2009), a minor alteration is required. Consequently, for the purposes of this thesis, outer space security is defined as: 'the secure and sustainable access to, and use of, outer space, whereby an entity is confident that any unreasonable (unjustified) dangers or risks they identify as threatening to their outer space infrastructures have been sufficiently mitigated against'. This definition places an emphasis upon the dangers and risks that each individual actor considers threatening, meaning that an issue which concerns one entity may not be of equal importance to another. Additionally, there is an implicit acknowledgment that any identified dangers or risks may well never be entirely negated, although it is possible to mitigate them to an acceptable extent (see Krepon *et al*., 2011: 4). This applies to many issues of concern for spacefaring entities, but particularly to the space debris population, which is steadily growing with, at the time of writing, no apparent short- or long-term solution(s). Moreover, the emphasis on outer space infrastructures indicates the need for the security of all segments associated with extra-terrestrial operations, including ground and space segments and the connectivity between them.

This thesis approaches outer space security through a broadly critical constructivist perspective; it conceives of security as a concept dependent upon risk and dangers – military and non-military – that individual actors perceive as being threatening to themselves or their activities. Campbell (1998) contends that "[d]anger constitutes more than the boundary that demarcates a space; to have a threat requires enforcing a closure on the community that is threatened. A notion of what 'we' are is intrinsic to an understanding of what ‘we’ fear” (p. 73). The ‘we’ in question in the context of this thesis is the EU, which is identified in chapter 2 as an entity with a desire to consolidate its status as an influential actor in outer space affairs. As is discussed in chapter 2, the EU’s space policy priorities revolve around enhancing regional and external initiatives in areas such agriculture, transport, humanitarian aid and the Common Security and Defence Policy (CSDP), encouraging investment in European space programmes and associated projects, and securing independence from other space actors with respect to some critical services, such as GNSS signals (Council of the European Union, 2011; European Commission, 2011b: 3). Therefore, in terms of outer space activities it can be argued that the EU’s ‘fears’ will relate mostly to the disruption of the services provided by its Earth-orbiting assets and the impact this may have upon its policies and the European economy.

As noted above, the definition of outer space security applied by this thesis emphasises the importance of entities identifying dangers or risks that they perceive as threatening. The act of identifying risks and dangers as threats discursively constructs a security identity specific to the entity performing the act. It does not have a direct effect upon the objective existence or nature of those risks and dangers, nor does it affect the existence of ones not deemed threatening. This designation does however transform the subjective existences of those risks and dangers, as perceptions of them change, and it is these subjective existences which inform an entity’s security identity. This is particularly relevant in relation to the extra-terrestrial environmental dangers discussed in chapter 5; the objective existences of space debris and space weather are not tempered by the extent to which an entity considers them threatening. Rather, the prioritisation of some dangers above others shapes the measures an entity undertakes to enhance its security. Consequently, this thesis looks to contribute to EU policy debates by investigating the risks and dangers which the EU perceives as being threatening to the security of its critical outer space infrastructures and analysing the means through which it seeks to mitigate those threats.

1.5 Scope, limitations and methods

This thesis analyses the means through which the EU is attempting to secure the space segments of its critical outer space infrastructures. The criteria used by the EU to identify critical infrastructures will be discussed in more detail in chapter 3 and the case studies used will be the EU 'flagship' programmes: the Galileo and Copernicus projects. The use of case studies in research projects is valued, as it “provides an opportunity for one aspect of a problem to be studied in some depth” (Bell, 2005: 10). Case studies offer an insight into on-going projects or programmes, in this case Galileo and Copernicus, enabling the analysis of present day practice which provides a platform for a comparison between practice and theory which would be difficult to accomplish through other methodologies. While there is some criticism of the case study methodology for placing too much emphasis on a single aspect (Bell, 2005: 11; Bryman, 2008: 55), the use of case studies is considered pertinent for the purposes of this research project as they offer a means of analysing the implementation of policy in practice.

The focus of this thesis is firmly upon the security of the space segments of critical outer space infrastructures. While ground segments are integral to outer space infrastructures and their security crucial, the author is of the opinion that incorporating an analysis of the credible risks and dangers to ground segments into this research project would have expanded it beyond a manageable level, particularly given the notable differences between many threats to ground and space segments, and efforts to mitigate them. Taking environmental factors as an example, while space segments are particularly vulnerable to space debris and radiation space weather events (SWEs), ground segments may well be at risk of damage from terrestrial meteorological and geological phenomena. In terms of intentional threats, the dangers facing ground segments are geographically and geopolitically contextual; depending upon their location on the globe, elements of ground segments may be at a higher risk of certain environmental factors or political instability threatening the bilateral agreements between the host state and infrastructure owner. Although ground and space segments are both crucial to outer space infrastructures, there is sufficient distinction in terms of their functions to separate them for the purposes of analysis. The category of ground segments commonly includes launch facilities, signal receivers and control stations, whilst space segments are, for the purpose of this thesis, defined as any objects launched into a self-sustaining orbit beyond the Kármán line and designed to conduct extra-terrestrial operations. Given the variables involved in the security of ground segments, the security of the EU’s outer space infrastructures’ ground segments deserves a thorough in-depth analysis which is beyond the scope of this thesis.

Where relevant, other outer space programmes, such as weather and remote sensing satellites, are also included within discussions, though these are supplementary with the focus remaining on Galileo and Copernicus. In addition, for the sake of comparison and comparative analysis, the policies of other major spacefaring actors are occasionally discussed, most notably, in chapter 4 with regards to the militarisation and weaponisation of outer space; although the issue is pertinent to the EU’s diplomatic endeavours with regards to the draft International Code of Conduct for Outer Space Activities, it does not have an overt military capacity of its own.

The overall objective of this thesis is to identify and analyse the EU's approach to outer space security, however it must be noted from the beginning that confidentiality has limited access to numerous EU and ESA documents as well as restricted the recording and discussion of some topics during interviews. For instance, the risk assessments for both

Galileo and Copernicus are, unsurprisingly, some of the most confidential documents at ESA (Anonymous, 2012a). Consequently, where possible this thesis refers to policy and technical documents specific to Galileo and Copernicus but elsewhere, the author has based his arguments on publicly available recommendations, guidelines and standards on topics such as physical protection measures, built-in redundancy and the priority of risks which infrastructures are being protected against.

Following the methodological precedence set by Lobo-Guerrero (2012a) and Suzuki (2003), the research for this thesis was a three-stage process, incorporating empirical research using primary documents and interviews alongside academic literature. Although it may have been possible to undertake this research project using solely primary documents and existing academic literature, the information obtained through the interviews provided insight and more in depth understanding of issues and procedures, which underpinned the analysis process and also included technical perspectives not found in other written sources. The three stages of the research project were not cyclic but closer to iterative, often informing each other insofar as issues of interest would emerge which would then shape interview questions or require the revisiting of particular documents or literatures.

The analysis of documents is an important aspect of social science research (Prior, 2003: 3) and is particularly pertinent to this project as many of the debates surrounding European outer space policy have been recorded in this format. Whilst it is has been proposed that there is an important differentiation to be made between records and documents, with the former being official written texts and the latter pertaining to personal ones (Hodder, 2003: 156), for the sake of simplicity both are referred to as ‘documents’.

This research project takes a “‘problem-oriented approach’” (Duffy, 2005: 123) to the analysis of archival documents, insofar as the author has reflected on the reading of secondary sources to inform the empirical research whilst bearing in mind both the project’s research questions and the need to ‘wonder’ (Lobo-Guerrero, 2012b; Guillaume, 2012). This approach permitted the author to develop an understanding of the subject area as documented before proceeding to the analysis of primary sources, focusing the research and enabling a critical analysis of the content and context of the documents.

This thesis analyses the information and data compiled through the research process through the broadly critical constructivist approach mentioned earlier, with the ultimate objectives being to identify the risks and dangers which the EU perceives as being threatening the security of the space segments of its critical outer space infrastructures and assess the measures taken in response to those threats. In taking this approach, it frames European outer space security efforts as forms of anticipatory security mechanisms highlighting both the prioritisation of risks and dangers by the EU as well as underlying European conceptualisations of extra-terrestrial security.

The research project began with an extensive literature search of existing debates and discourses regarding European outer space security. For the empirical research, a number of policy and technical documents originating from a wide range of sources were compiled, including but not limited to the Council of the European Union, the EC, ESA, the Consultative Committee for Space Data Systems (CCSDS) and the UN. These sources were chosen for specific reasons; for instance, as the executive arm of the EU the EC publishes proposed communications and working papers concerning European outer space activities and programmes proposed to the Council of the European Union and the European Parliament for approval.

As the agency charged with procurement for a number of European outer space programmes, including Galileo and Copernicus, ESA produces and publishes documents and information concerning the architecture and objectives of these programmes.

Moreover, ESA is actively involved in on-going research into space debris and space weather and is, at the time of writing, managing the space weather and Near-Earth Object segments of the European Space Situational Awareness (SSA) programme.

The CCSDS is a forum founded by space agencies in 1982 (Consultative Committee for Space Data Systems, 2013a) and currently has 11 member agencies.[11] It creates and publishes recommendations for public release concerning data systems in order "to promote interoperability and cross support among cooperating space agencies, to enable multi-agency spaceflight cooperation […] and new capabilities for future missions" (Consultative Committee for Space Data Systems, 2013a). Given that the CCSDS comprises of some of the most active and experienced national and international space agencies, there is good reason to assume that the issues and recommendations discussed in its publications are attributed similar importance by those individual agencies. Consequently and of particular relevance to this thesis, while not specific to either the Galileo or Copernicus programmes, the security measures recommended by the CCSDS in its publications are indicative of the possible direction of internal and confidential discourses over the security of European critical outer space infrastructures.

Last but not least, the UN publishes existing international law, such as the 1967 Treaty on the Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies,[12] as well as documents emerging from its organs, including the UN Office for Outer Space Affairs (UNOOSA) and its associated sub-committees. In addition, the UN Secretariat is the body with which

---

[11] These are the Agenzia Spaziale Italiana (ASI), the Canadian Space Agency (CSA), the French Centre National d'Études Spatiales (CNES), the Chinese National Space Administration (CNSA), the Deutches Zentrum für Luft- und Raumfarht e. V. (DLR), ESA, the Brazilian Instituto Nacional de Pesquisas Espaciais (INPE), the Japan Aerospace Exploration Agency (JAXA), NASA, the Russian Federal Space Agency (RFSA) and the United Kingdom Space Agency (UKSA) (Consultative Committee for Space Data Systems, 2013b).

[12] Hereinafter referred to as the Outer Space Treaty (OST).

states party to the 1976 Convention on Registration of Objects Launched into Outer Space[13] are requested to register outer space objects.

Close attention has been paid to the need to maintain an awareness of the context of documents and archival records, permitting engagement with the imaginaries which underpin them (see Lobo-Guerrero, 2012a). All the documents collected for this thesis have been approved for public access and are mostly available online. As mentioned above, a number of documents pertaining to the security of Galileo and Copernicus remain confidential and thus unattainable for the research conducted in this project. Both the volume and nature of the information which remains confidential is unknown to the author, and consequently the validity of the arguments made and conclusions reached within this thesis is predicated upon the documents and information that has been approved for public release by the EU, ESA, CCSDS and the UN. Whilst this may be problematic in terms of the scope of the research conducted, as it means that the thesis is dependent upon information that the aforementioned institutions have deemed acceptable for public digestion, the research design of combining existing academic literature, documentary analysis and semi-structured interviews has enabled feasible analysis of the subject matter.

For the final stage of the research process, semi-structured interviews (n = 7) were conducted with experts working at the EC, ESA and the UKSA. According to Bryman (2008), “[t]he interview is probably the most widely employed method in qualitative research” (p. 436). The justifications for semi-structured interviews, in contrast to structured interviews, is that the former focus more on the opinions of the interviewee and are far more flexible (Bryman, 2008: 437-438). The interview participants were identified because of their experience and knowledge of the issues and programmes that this thesis is concerned with, and their knowledge and assistance has been invaluable to the research

---

[13] Hereinafter referred to as the Registration Convention.

project. Although some of the participants were employees of the same institution, their areas of expertise were different, and the content therefore furthered both the understanding of the issues and processes but equally offered either contrasting views and opinions to be considered or supportive reflections. These interviews enabled coverage of a variety of subjects yet permitted general questions regarding wider institutional policy-making to be posed for comparison. While the majority of the participants did not have English as their primary language, their knowledge of English, combined with the fact that much of their work is conducted in English, meant that there were very few linguistic issues during the interviews.

Since this project is investigating the security of the EU's critical outer space infrastructures, much of the discussion will be oriented towards the decisions and discourses of European institutions, specifically the Council of the European Union, the EC and its associated Directorate-Generals and, last but not least, ESA. These agencies are fundamental to the formulation of initiatives, mechanisms and policies oriented towards the security of European critical outer space infrastructures. However, on occasion comparisons with non-European practices or conceptualisations are relevant in order to provide context for debates taking place in Europe. This occurs twice in the thesis to a notable extent; firstly in chapter 3 with regards to the definition of critical infrastructures by the US Department Homeland Security (DHS) and the origins of Critical Infrastructure Protection (CIP) in the 1997 President's Commission on Critical Infrastructure Protection (PCCIP). The second instance, in chapter 4, concerns the military space programmes of the US, the Russian Federation and the People's Republic of China (PRC). As the EU appears to show no interest in developing a space weapons programme of its own, an overview is provided of these three countries' ASAT programmes to illustrate the capabilities of existing technologies in this field.

Following the overview of existing and past ASAT programmes, there is a discussion of US doctrine concerning military space applications. Again, the purpose of this is to provide context and contrast to the relatively non-military approach undertaken by the EU, as well as highlighting the importance of international efforts to prevent the weaponisation of outer space. The decision to focus solely on US military outer space doctrine was based upon two factors; firstly a desire to provide some context without digressing too far from the European focus of the research project, and secondly the linguistic abilities of the author. Although some documentation on Russian and Chinese military space doctrine is available, it was considered that this was beyond the required scope of this thesis and that the time and resources required verifying possibly unreliable translations of government and military documents would detract from the focus of the research project.

1.6 Thesis structure

This thesis is split into six substantive chapters, including this introduction, analysing the EU's ambitions in outer space, critical infrastructures and the Galileo and Copernicus programmes, intentional threats to outer space infrastructures and environmental hazards facing satellite networks.

The next chapter explores role of the EU in the coordination and management of pan-European outer space activities. It begins by introducing the hierarchy of actors present within EU outer space activities. Outer space policy-making at EU level is reflective of its terrestrial policies, in terms of equal access to space and the increasing use of outer space systems to complement and enhance spatial projects, along with European internal and external security. To this end, outer space infrastructures are framed as a means of policy-multiplication, making them examples of a regional and global European space power projection. The chapter concludes by examining the objectives of the EU’s outer space policy, and its evolving relationship with ESA.

The third chapter explores the EU’s labelling of its outer space assets as critical infrastructures. It offers a brief history of efforts to secure critical infrastructures, from the emergence of CIP to the evolution towards CIR, whereby resilience and redundancy are considered equally important to attempts to deter threats. The conceptual framework of anticipatory security is introduced before being developed further in the context of outer space security in subsequent chapters. Building upon on the arguments made in the second chapter, the third chapter contends that satellite constellations and the services they provide fulfil the requirements to be included amongst critical infrastructures and European Critical Infrastructures, although they are very rarely acknowledged as such in public. Finally, the two European flagship outer space programmes, Galileo and Copernicus, are outlined and framed as examples of future European critical outer space infrastructures. Some background will also be provided on programmes and technologies relevant to these projects to place Galileo and Copernicus within the wider context of European and international efforts to explore and exploit the domain of outer space. The chapter concludes by arguing that the future importance of the Galileo and Copernicus programmes to European societies makes their protection a matter of necessity.

The fourth chapter begins by differentiating between the militarisation and weaponisation of outer space, arguing that whilst outer space is already militarised, it has not yet been weaponised. It then offers a brief history of the development of ASAT systems and technologies as background to the on-going debates over the weaponisation of outer space. As the US has undertaken the most research into ASAT technologies, the military doctrine underpinning its space policies are also discussed in order to highlight the importance of outer space operations to military strategists and justify why counterspace operations may be prominent in any future conflicts between spacefaring actors. The chapter then analyses the extent to which on-going efforts to prevent intentional man-made threats to outer space infrastructures, and in particular the draft International Code of Conduct for Outer Space Activities championed by the EU, are advocating sustainability through practices predicated upon logics of preemptive anticipatory security.

The fifth chapter outlines the ‘natural’ environmental phenomena, namely space weather and near-Earth objects, which have the potential to damage or destroy man-made assets in outer space before turning to the issue of space debris. The means undertaken by the EU and its affiliated agencies to counter and mitigate the effects of extra-terrestrial environmental hazards are analysed in the framework of anticipatory security. Many risks that are being countered or mitigated are already proving dangerous to on-going operations and thus, although there is an element of sustainability at play, the measures discussed in this chapter are designed to secure the present as much as the future. As well as framing the European SSA as an anticipatory security mechanism, there is also discussion of the extent to which existing responses to extra-terrestrial environmental risks conform to terrestrial critical infrastructure resilience or protection strategies.

2 Europe and outer space

Before matters relating to the security of European outer space infrastructures can be discussed in any great detail, it is necessary to outline European outer space activities; the actors involved, the motivations behind independent European outer space capabilities and the history of those capabilities.

With the exception of some scientific missions and probes, the majority of outer space assets and technologies are designed to complement and enhance terrestrial policies, objectives and infrastructures. The European Union (EU) is making an effort to highlight this relationship between terrestrial societies and outer space, along with the integral role outer space assets play in its regional policies. As mentioned at the beginning of the first chapter, the EU Space Expo has been touring Europe in 2012 and 2013, explaining through audio-visual presentations how outer space assets and technologies benefit European societies and individuals. The exposition ties in with recent EU efforts to establish the close relationship between outer space and individual Europeans; a 2011 Communication from the European Commission (EC) was titled "towards a space strategy for the European Union that benefits its citizens" (European Commission, 2011a: 1). Moreover, 2013 has been declared the 'European Year of Citizens' (see Europa.eu, 2013), an event ostensibly dedicated to informing and reminding Europeans of their rights as EU citizens but which will likely have the consequence of portraying the ways through which the EU is integral to European societies. Although there is no direct link between outer space assets and technologies and the 2013 European Year of Citizens initiative, it could be argued that the similar foci on individual benefits indicates that the EU is making a concerted effort to incorporate outer space affairs into its wider terrestrial policy-making.

This chapter explores role of the EU in the coordination and management of pan-European outer space activities and the reasons behind the perceived need for independent outer space capabilities. The chapter begins by introducing the hierarchy of actors present within EU outer space activities and then explores the concept of power projection and how it complements space power. Outer space policy-making at EU level is reflective of its terrestrial policies, in terms of equal access to space and the increasing use of outer space systems to complement and enhance spatial projects and European internal and external security. To this end, outer space infrastructures are framed as a means of policy-multiplication, making them examples of a regional and global European space power projection and thus central to European ambitions in terms of outer space affairs. The chapter concludes by examining the objectives of the EU's outer space policy, and its evolving relationship with ESA.

2.1 Actors in European outer space activities

There are numerous actors involved in outer space activities, from states to national and multinational corporations (Jakhu and Singh, 2009: 77). State-operated satellites are commonly dedicated to military, government or scientific use, while commercial satellites are often providers of telecommunication or remote sensing services. As with many areas of international relations, states are arguably some of the most important actors, particularly given that they are responsible for satellites launched and operated under their name. Although there are many commercial satellites in orbit operated by national or multinational corporations, such as Intelsat, existing international law places responsibility and liability firmly with the launching state. Nonetheless, with regards to the outer space activities of the EU, a state-centric framework would offer an inadequate and incomplete analysis (Suzuki, 2003).

Concerning European outer space activities, the EU has seen its role in policy-making increase in recent years, particularly since the signing of the Lisbon Treaty in 2007, which established European space policy as being a "*shared* competence of the EU" (Mutschler and Venet, 2012: 118, original emphasis) in Article 189. The emphasis on shared is important, as regional outer space policy-making in Europe involves three tiers of actors: the EU, ESA, and Member States (both of the EU and ESA[14]), including their respective national space agencies. The involvement of the EU and ESA Member States is mostly related to funding and policy-making, which set the priorities for the development of pan-European outer space programmes and associated projects and applications, even if there continues to be some variation in domestic policies and objectives. Suzuki (2003) has charted the complex relationship of collaboration between the EU and European states since 1960, concluding that

> [t]he history of European space collaboration reminds us that even though European governments could not strike a balance in their policy logics, they innovated new institutional arrangements to accommodate those logics under a European umbrella. After all, the European governments knew that they would not accomplish the level of technological expertise and competence in space if there was no collaboration (p. 213).

---

[14] The Member States of the EU and ESA are not identical; Canada, Norway and Switzerland are members of ESA but not of the EU, whilst not all Member States of the EU are members of ESA. This has created friction between the organisations, which is discussed later in this chapter.

Collaboration between states and their space agencies is a necessary component of European outer space activities. Individually, European states lack the financial, industrial and scientific resources to develop large-scale space programmes capable of challenging those of the US, Russia and, in the future, China.

Taking the Galileo and Copernicus programmes as examples, a number of bodies of the EU have different roles within their development and management; although not at the time of writing an organ of the EU, ESA is responsible for the design and procurement of the ground and space segments for both programmes. Meanwhile, the EC is tasked for the overall funding and management of Galileo and Copernicus, with some governance over specific issues delegated to dedicated organisations such as the European GNSS Agency (GSA), which is responsible for the Public Regulated Service (PRS) and signal security of the Galileo programme. The projects and applications developed for the services that Galileo and Copernicus provide are mostly funded by the EU, under the 7th Framework Programme for Research (FP7) and the Horizon 2020 programme,[15] or by ESA. These projects and applications are discussed in more detail in chapter 3 of this thesis but for the moment it must emphasised that their management is largely separate to that of the programmes themselves.

2.2 Power projection and outer space

The services provided by satellites are arguably forms of global power projection from outer space. Projection, particularly power projection, is inherently geopolitical (Williams, 2010; 82-84; 2011: 254). It reflects a sense of space and place, whereby power is enforced and performed ‘over there’, as opposed to at the heart of the entity undertaking

---

[15] In 2013 the EU launched Horizon 2020, the successor to FP7 covering research activities between 2014 and 2020 (Council of the European Union, 2013).

the projection (‘over here’). This spatial separation between ‘here’ and ‘there’, a form of geographical ‘othering’ (see Said, 1993: 54; P. E. Steinberg, 2001: 36-37), also enables projection by providing it with a location. However, projection is not power, it is a ‘means’; a link in the chain of events that begins with an effect being imposed upon something/someone in a different spatial location to the entity from which the effect emanates. There are numerous ways in which projection is performed, from the video projector, which projects light across a space onto a standing structure, to military power, enforced upon an unfriendly community or state through multiple means, such as airstrikes, embargoes and pitched battles. While the effects of projection have been subject to rigorous scholarly study, the act itself has proved less popular amongst academics.

2.2.1 Projection as an instrument of power

To begin with, however, it is worthwhile establishing what is intended by use of the word ‘power’ in the term ‘power projection’. For better or for worse, there are numerous debates over the definition of ‘power’. Berenskoetter (2007) notes that even within the discipline of International Relations, “‘power’ is an essentially contested concept, with different interpretations held together more by a family resemblance than a core meaning” (p. 1). For example, in classical strategic thinking, it has been argued that military power “refers to the capacity to kill, maim, coerce and destroy” (Garnett, 1975: 50), while Agnew (2005) notes that “[i]n the modern geopolitical imagination, power has been defined as the ability to make others do something you desire” (p. 51). Meanwhile, according to Foucault (2009), power relates purely to domination or subjection (p. 156). In her study of violence Arendt (1970) describes power as “the human ability not just to act but act in concert” (p. 44); in this manner power is conceived as a collective socio-political phenomenon, whereby “[w]hen we say of somebody that he is ‘in power’ we actually refer to his being empowered by a certain number of people to act in their name” (p. 44). Arendt argues that:

> [p]ower needs no justification, being inherent in the very existence of political communities; what it does need is legitimacy. […] Power springs up whenever people get together and act in concert, but it derives its legitimacy from the initial getting together rather than from any action that then may follow (p. 52).

This being said, Arendt also acknowledges the common usage of the term power metaphorically to denote ‘strength’ (p. 44).

The variance in definitions of power highlighted above is due in no small part to the subjectivity of the topic. As Lukes (2005) warns:

> power is one of those concepts which is ineradicably value-dependent. […] [b]oth its very definition and any given use of it, once defined, are inextricably tied to a given set of (probably unacknowledged) value-assumptions which predetermine the range of its empirical application (p. 30).

According to Lukes, then, the meaning of the term ‘power’ is limited by the context in which it is used. Consequently, on the subject of this chapter, ‘power’ and ‘power projection’ are interdependent variables; while a specific type of ‘power’ may influence the means of projection (for example, military power projection over great distances necessitates a certain set of technologies), those same means of projection arguably have a significant impact upon the character of the projected power, as technological limitations affect the effectiveness and influence of the projecting entity's power. Moreover, returning to Arendt's (1970) point on the need for power to have legitimacy brought about through consensual group recognition, the instruments used to provide that legitimate empowerment can reveal some of the projecting entity's underlying values. For instance, the decision to project 'power' through military or non-military means may be indicative of the projecting entity's objectives or willingness to use force to achieve the desired legitimacy. In addition, the consensual group recognition of an entity's power occurs both internally and externally. The existence and legitimacy of the EU's space power needs to be acknowledged internally by EU Member States and externally by other spacefaring actors such as the US, the People's Republic of China (PRC) and the Russian Federation amongst others. Dual recognition is necessary because although the instruments of the EU's space power are being applied externally – insofar as the EU as an institution does not always directly receive the benefits of those instruments – as a politico-economic union the EU requires internal legitimacy to function effectively. This is particularly important in the context of outer space activities, given that many EU Member States maintain independent space programmes distinct from collaborative European initiatives.

Finally, it must be noted that there is not a single overarching 'power'; rather, as Foucault (2009) states when commenting on Marx's deliberations on the subject; "there exists no *single* power, but several powers. […] We cannot therefore speak of power, if we want to do an analysis of power, but we must speak of powers and try to localize them in their historical and geographical specificity" (p. 156, original emphasis). This applies as much to power projection as it does to power generally: the projection of cultural power through globalisation for example, takes place simultaneously alongside (and largely independent of) other forms of power projection, such as US manned and unmanned fighter missions across the globe. With regards to space power, as Peter (2010) comments, "[i]t is not a single property, but a combination of factors. Space power is composed of a set of interrelated elements. It is not simply satellites and launchers. It is anything and everything a country can achieve through space" (p. 351). In other words, space power stretches a number of spheres – including commercial, economic, military, scientific and technological – and can be associated with all activities an actor undertakes related to outer space.

2.2.2 Power projection without violence

Given its geopolitical intonations, military power projection may be one of the most popular forms of study in the discipline of International Relations, but is by no means the only one worth considering in relation to outer space. The history of cultural, colonial and, to a lesser extent, imperialist projections offer an insight into means by which power has been applied indirectly outside of a state's borders, and provides the foundation for a framework for the analysis of contemporary power projections originating from outer space infrastructures. In the context of this thesis, power projection includes a wide range of technologies and means of projecting power with the objective of establishing or expanding the legitimacy of an entity's power. The discussion that follows is intended to highlight some of the means through which non-military power projections are manifested. The ultimate objective here is to demonstrate the means through which European outer space programmes are representative of a peaceful power projection seeking to establish Europe's legitimacy as a leader in outer space affairs.

Edward Said (1993; 2003) discusses, at length, global projections of culture emanating from Western Europe and the US. In particular, he proposes one of the most well-known examples of cultural projection: Orientalism. This concept revolves around the argument that European cultural undertakings, be it art, academic thinking or literature dating from Ancient Greece to the 20th Century, ontologically and epistemologically 'created' the Orient in a particular manner, attributing to it the values and dangers that Europeans *wanted* to see (Said, 2003). They were, essentially, projecting their preconceptions of the Orient upon the region, even if the reality was quite different.[16]

Perhaps more importantly however, Orientalism had a secondary effect, whereby "European culture gained in strength and identity by setting itself off against the Orient as a sort of surrogate and even underground self" (Said, 2003: 3). Thus while European culture was on the one hand 'creating' the Orient, it was simultaneously being 'created' by that same process. This self-constituting process was not, however, limited to European cultural projections. In *Culture and Imperialism*, Said (1993) widens his parameters in an attempt to account for the pattern of global cultural imperialism emanating from Europe and North America in recent decades. Furthermore, such imperialist influences remain today, albeit under the euphemism of cultural globalisation.[17]

While the origins of the global cultural imperialism studied by Said (1993; 2003) began perhaps as early as the writings of Hellenic Greece (Said, 2003: 56), colonialism provided Europeans an opportunity to expand their influence and, simultaneously, their cultures (see Parry, 1973; Seed, 1998). Abulafia (2008) and Sokolow (2003) note that the 'discovery' of the New World quashed numerous rumours about distant peoples (Abulafia, 2008: 14; Sokolow, 2003: 55), yet those same discoveries provided an opportunity for the Europeans to project their cultural legacies upon expansive 'new lands' and 'less-advanced' populations (Abulafia, 2008: 5). Take, for example, Christopher Columbus' naming of islands in the New World as a means of establishing possession over said

---

[16] As Said notes in the preface to the 2003 edition of *Orientalism*, this state of affairs has not changed greatly in recent years, with attempts to impose regime-change in Middle Eastern states characterised by historical and cultural naivety (see Said, 2003: xii-xv).

[17] See for example, Caldicott and Eisendrath's (2007) chapter on the importance of outer space, where the global projection of American entertainment and moral values through satellite telecommunications is argued to be one of the most important features of satellite networks.

islands, despite the fact he was aware that they already had names (Todorov, 1992: 27-28). It could be argued that the placement of the US flag on the Moon by the 1969 Apollo 11 mission evokes a similar mentality of symbolic possession, despite the fact that the Outer Space Treaty (OST) prohibits the national appropriation of celestial bodies.

Columbus' actions epitomised a European colonial mentality characterised by the perception of indigenous populations as 'inferior' to the colonisers. While the technological superiority of the Europeans certainly played a part in this discrimination (Wright, 1992: 6-7), religious values were also an important consideration (Parry, 1973; Sokolow, 2003; Todorov, 1992: 10); Abulafia (2008) points out that Ferdinand V of Aragon was determined to "bring Christianity to the whole world" (p. 11). Colonialism, therefore, was not only a cultural and territorial affair but also one of religion, where the projection of Christianity across 'heathen' lands was considered of the upmost importance (Sokolow, 2003: 39). This territorial expansion and projection of religious and cultural values was assisted by contemporary international law, which, as Schmitt (2006) contends, portrayed the New World as divorced from Europe and therefore a quasi-*terra nullius* (p. 130), justifying it being open to appropriation by the European explorers in the name of 'discovery' (p. 131).

More recent examples of power projection exist as well. Williams (2010) explores the geopolitical influence of the trans-Pacific air route established by Pan Am in the 1935, which necessitated the construction of commercial aviation facilities on islands across the Pacific. While the 1922 Washington Naval Treaty prevented the construction and upgrading of military facilities on US territorial possessions in the Pacific Ocean, it did not preclude civilian air bases (Williams, 2010: 88-89). Consequently, the US was able to covertly extend its presence across the region in a manner "legitimised in the form of a commercial airline" (Gandt, 1991: 74, cited in Williams, 2010: 89). Williams concludes that the Pan Am trans-Pacific air route firmly established numerous Pacific islands, including Wake and Midway, as US sovereign territories in the minds of the American population, further galvanising the public outcry following the attacks on Pearl Harbour and other US possessions in December 1941 (p. 96). The Pan Am example highlights the importance that commercial ventures can play in the projection of state power and influence, arguably existing in the early 21st Century through commercial globalisation. While multinational companies may not have direct links to the government of the state in which they began, there is often a cultural connection. Taking McDonalds and KFC as examples, they have both exported a way of cooking and serving food which is arguably portrayed, either consciously or subconsciously, in written and visual media as epitomising the American way of life. Therefore, although the US government does not have an overt presence in towns and cities around the world, its companies are constantly reminding customers of the US's global commercial influence.

There is another form of power projection which does not require the displacement of troops or material across the globe; the transmission of power through visual media. Photography has been used since the 19th Century for the purposes of domestic and international propaganda; for example, on the orders of Stalin, Trotsky was famously airbrushed out of a photo of a communist rally in the Soviet Union, while the Nazi government in Germany created the *Reichsministerium für Volksaufklärung und Propaganda* (Ministry of Public Enlightenment and Propaganda) in 1933. In the early 21st Century, the proliferation of near-instant communication through the internet has made visual media even more influential and widely-available. Taking as an example the bombing of Baghdad during Operation Desert Storm and Operation Iraqi Freedom by coalition forces, the numerous images (both photographic and cinematographic) served to remind those watching of the military might of the US and its allies. Visual representations of state power may not be a direct form of power projection – it will not destroy a building or topple a government – but it nevertheless acts as an affective transmission of power to populations worldwide.

Equally, terrestrial populations have been bombarded with the possibility and potential of space weapons through various forms of multimedia (Johnson-Freese, 2009: 20-22). These include computer and console games (such as *Sins of a Solar Empire*, where the player is able to construct static defences based in a planet's orbit to defend it against attack, and the *Red Alert* series, where players can construct space-based weapons capable of destroying any terrestrial unit) and films (such as *Goldeneye*, *You Only Live Twice* and the infamous Death Star of the *Star Wars* films). Consequently, the notions of space weapons and power projection in and from the domain of outer space are not completely alien to modern societies. This is significant, as the importance of film in astropolitical and geopolitical thinking must not be underestimated. Carter and McCormack (2010) discuss the affective nature of imagery and its influence upon and reflection of geopolitical culture, taking as examples *The Thin Red Line*, *United 93* and *Three Kings*. They conclude that films:

> are important not only insofar as they provide geopolitical texts to be decoded and deconstructed. They can and should also be understood as critical-geopolitical thinking-spaces in which we might explore how images participate in geopolitical cultures (pp. 119-120).

Consequently, the normalisation of space weaponry through computer games and visual media should not be easily dismissed. While those knowledgeable in outer space affairs may well be aware of the dangers posed by space weapons and the current financial and technological obstacles preventing their mass-production, consumers have been shown films where some satellites capture or destroy spacecraft and others beam deadly lasers capable of demolishing buildings. Equally, the panoptical qualities of surveillance satellites have been affirmed endlessly in films and games, from *Enemy of the State* and *Patriot Games*, where satellites are capable of streaming live video feed at extremely high resolutions, to the *Civilization* series of computer games, where access to space is rewarded by an unrestricted view of the Earth and the movement of all other players' units. The technological accuracy of the aforementioned films and games is not debated here[18] but, as Carter and McCormack (2010) argue, when commenting on popular geopolitics, it is important to consider the affective nature of visual media and imagery. In the case of space weapons, consumers have been bombarded with so much imagery and postulation that it would be of little surprise if popular thinking leant towards the existence of operational space weapons.

Furthermore, the portrayals of space weapons in the aforementioned games and films are bordering on the romantic: whilst the capability of such systems to destroy or capture other satellites is shown, the long-term effects, such as space debris, are not. Space weapons are shown to be surgical in their precision, arguably representative of widespread hopes that "[s]pace technology promises to offer an automated, clean and sanitised mode of destruction and killing" (Bormann, 2012: 78). Although this may appear relatively trivial, it means that the task at hand for opponents of space weapons is considerably harder as, at least on reel, outer space is already weaponised. Consequently, efforts to sway public opinion away from space weapons may meet an opposition educated by the relatively romantic portrayals, where the separation between reality and fiction has been

---

[18] For a discussion on the inaccurate portrayals of satellite capabilities in films, see Johnson-Freese (2009: 66-69)

blurred. Space weapons and the military applications of satellites are discussed in greater detail in chapter 5 of this thesis, but at this point it is relevant to emphasise the subtle normalisations of technological futures that can emerge – intentionally or accidentally – through media often transmitted by satellites.

Whilst highlighting that power projection is not directly restricted to military subordination (see Russell, 1994; Simmel, 1994), the aforementioned examples also offer evidence of how such non-military power projections occur and have occurred. They are still relevant when considering outer space affairs, as modern satellite-based telecommunications offer the opportunity to project entertainment and media across the world; in one way de-territorialising the Earth by abstracting geographical distances, yet simultaneously reinforcing the statist divisions of the globe by constantly reminding populations of cultural and moral differences.[19]

2.3 The origins of European collaboration in outer space

The early years of European collaborative outer space activities were characterised by a focus on civilian and scientific pursuits. Up until 1960, outer space research within Europe had been conducted independently by states, and it was only after the International Geophysical Year in 1957 and the establishment of the Organisation Européenne pour la Recherche Nucléaire (CERN) in 1954 that support began to grow for collaboration on European space programmes as well (Krige and Russo, 2000; Suzuki, 2003: 40-41). The efforts of two physicists – the Italian Edoardo Amaldi and the French Pierre Auger – through 1959 and 1960 have been described as pivotal in the establishment of the first European organisation dedicated to outer space research; Krige and Russo (2000) go so far

---

[19] One only needs to browse the diverse range of channels available on digital television in the UK to notice the plethora of channels dedicated to religion (for example, the God channel) and culture-specific entertainment (for example, FX, Sky Atlantic, Bollywood).

as to propose that they could be considered the “founding fathers” (p. 22) of European collaboration on outer space.

In 1964, the European Space Research Organisation (ESRO) Convention came into force, and the organisation was founded. ESRO’s competency was restricted purely to scientific matters, as the 1960 Meyrin conference, at which delegates from European governments had agreed to the foundation of the organisation, determined that launcher development and commercial applications would be handled by other institutions (Suzuki, 2003: 47).

There remained a desire amongst European scientists and governments to develop an independent launcher capability. However, the negotiations behind the creation of the European Launcher Development Organisation (ELDO) were more complex than those which had taken place regarding ESRO, not least because of a “lack of common policy logic amongst countries” (Suzuki, 2003: 48). However, in 1960, the British abandoned Blue Streak, its Intermediate Range Ballistic Missile (IRBM) project manufactured by De Havilland Propellers (Williamson, 2006: 75), and proposed a European launcher using Blue Streak and its second stage Black Knight (Suzuki, 2003: 48). After a series of negotiations,[20] the eventual result was the Europa launcher, based upon the British Blue Streak rocket for the first stage, the French Coralie, manufactured by Vernor GIE, for the second stage and the German Astris, constructed by Entwicklungsring Nord (ERNO), for the third stage. The French supported the suggestion and offered Coralie – originally the Cora experimental rocket – for the second stage of the proposed launcher (Pfaltzgraff and Deghand, 1968: 22; Williamson, 2006). However, there were problems combining the British and French stages, with the latter failing twice during testing in 1966, whilst the German rocket also proved unsuccessful in two 1968 test-flights (Russo, 2000; Sheehan,

---

[20] See Krige and Russo (2000) and Suzuki (2003: 48-51) for detailed accounts of these negotiations.

2007: 78). On the one occasion that all three stages functioned as intended, the payload was not released correctly and could not reach the objective orbit; that failed test proved to be the last flight of Europa-1. A second version of the Europa rocket, Europa-2, underwent testing in the 1970s but exploded three minutes into its first flight in November 1971 (Williamson, 2006: 77-78). The project was abandoned in at the ELDO Council in April 1973, a decision which, Suzuki (2003) notes, was effectively the end of ELDO, a launcher organisation which failed to successfully launch a satellite into orbit (pp. 78-79).

At its July 1973 meeting, the European Space Conference was tasked with drafting a convention for a single European agency dedicated to research and development of outer space technologies (Suzuki, 2003: 80). The ESA Convention, using the ESRO Convention as a foundation, came into effect in 1980, although ESA itself had been operating since 1975 (Krige *et al.*, 2000: 34-35). The Convention promotes coherence in European space activities, a focus on non-military outer space applications, and what Suzuki (2003) refers to as the "Europeanization" (p. 88) of outer space programmes, whereby member states would be encouraged to inform others of their projects and offer opportunities for collaboration to avoid duplication across Europe (Suzuki, 2003: 88).

2.4 European launch capability and space power projection

As mentioned above, launcher technology played an integral role in the early years of European outer space collaboration. Although ELDO and ESRO may have, to all intents and purposes, merged into ESA in 1975, European launcher technology has arguably flourished. There are two European launchers in operation at the time of writing; the heavy-lift Ariane 5 developed by Arianespace and the smaller Vega, a joint project between the Agenzia Spaziale Italiana (ASI) and ESA. In addition, following a 2005 agreement between ESA and the Russian Federation regarding increased cooperation on outer space activities, Russian Soyuz launchers have been launched from Arianespace's[21] facility in French Guiana (European Space Agency, 2005). The EU views independent access to outer space as a strategic necessity but has voiced concerns that the "relatively small and open domestic institutional market exposes the European launcher sector to severe peaks and slumps in the commercial market, putting the industry at risk" (European Commission, 2007b: 9). The future of European launchers has been a topical issue in recent years, and was high on the agenda of the 2012 ESA Ministerial Council, where investment was secured for the continued development of the Ariane 5 Mid-life Evolution (ME) and the Ariane 6 launchers (de Selding, 2013). As its name suggests, the Ariane 5 ME is an incremental development of the Ariane 5 launcher, designed to replace the existing heavy-lift variants by the end of the decade. The Ariane 6 meanwhile is intended to be the future replacement for the Ariane 5 ME and the Soyuz, and is currently in the preparatory stage of development.[22] A decision will be made in 2014 by the ESA Ministerial Council on whether full development of the Ariane 6 launcher should begin (European Space Agency, 2013a).

Although the futures of Ariane 5 ME and Ariane 6 remain uncertain, it is clear from the investment being made into their development that the EU and ESA perceive the continued need for an independent European launcher capability. On the one hand, this is a purely commercial decision, in that European space industry benefits from the investment and commerce that launcher development entails. Moreover, the continued success of European launchers portrays the European space industry in a positive light and does no harm to European ambitions for prominence in outer space affairs. On the other hand,

---

[21] Arianespace is a French company established in 1980 and charged by European states with the management and operation of Ariane launch vehicles and launches (von der Dunk, 2010).

[22] Concerns have been raised over the design of the Ariane 6, with critics arguing the current plans to have two solid-fuelled stages and an upper cryogenic stage do not offer enough "growth potential" (de Selding, 2013).

subtle power projections are arguably involved as well. The agreement between ESA and the Russian Federation for Soyuz launchers to be launched from the Arianespace facility in French Guiana is particularly relevant, as it promotes Arianespace – and by association, ESA and Europe – as the owner and operator of the ground infrastructure necessary for successful launches: in other words, Europe is not restricted by its geographical location. The Arianespace website proudly incorporates Soyuz within the 'launcher family' (Arianespace.com, 2013), breaking down the barriers of national origin for both Soyuz and Vega, but arguably portraying all three launch vehicles as distinctly European affairs. European space power then is projected globally; not only can Europe develop independent launch vehicles of its own, but it has the capability to launch them from South America and is a chosen launch operator for the Russian Soyuz vehicles.

2.5 The inevitable evolution: The militarisation of European activities in outer space

Although Europe's early ambitions in space were confined purely to scientific matters, there can be no denial that contemporary European activities in the domain of outer space may have some military applications. Moreover, discourse within the EU and ESA has slowly changed, with security issues becoming more prevalent within considerations for future space policies and programmes, to the extent that "[s]pace is now seen as an essential and strategic asset for European integration and for non-dependence in the current geopolitical context" (Peter, 2005: 266). The 2007 European Space Policy (ESP) firmly indicates the perceived opportunities for European outer assets to contribute to the Common Foreign and Security Policy (CFSP) (Council of the European Union, 2007: 3), whilst the 7th Space Council resolution goes so far as to acknowledge "the increasing dependence of the European economy and policies, in particular the Common Foreign and Security Policy, on space assets" (Council of the European Union, 2010: 9).

To Sheehan (2012), this evolution “represents a disappointing break with the idealism that underlay the initiation of collaborative European space activity” (pp. 184-185), although he acknowledges that “it does offer Europe a mechanism through which, in conjunction with the EU it can shape the evolution of policy in line with EU rather than NATO perspectives” (p. 185).

Slijper (2008) offers a particularly negative view of the militarisation trend emerging within European outer space activities, contending that the possibility for signals from Galileo and Copernicus to be used for military purposes means that those programmes must be considered to be military, rather civilian, in nature (pp. 34-35). Proceeding to focus upon Copernicus, he argues that the increasingly dual-use nature of the programme indicates that it is “slowly […transforming] into an important military asset to support future warfare by European and NATO partners” (p. 39). These arguments are problematic for a number of reasons: firstly, the contention that dual-use means military ignores the complexity of the issue at hand. If all dual-use systems were military systems, then a host of other satellites, including those operated by the European Organisation for the Exploitation of Meteorological Satellites (EUMETSAT) and other meteorological organisations, would certainly need to be classified as military assets as well. Slijper’s questions over the future unintended use of data from Galileo and Copernicus are not without foundation, but then the same concerns could be voiced with regards to any form of knowledge-provision. Kaplan (2009) charts and analyses the use of mobile communications and social networking in the planning, undertaking and reporting of the 2008 terrorist attacks on Mumbai. While those attacks demonstrate that such technologies are to some extent already militarised, a state of affairs that Kaplan argues requires “critical engagement rather than romanticization” (p. 310), the fact that they are dual-use does not make them inherently military in nature. The point here is that any number of sources of knowledge, technologies or systems can be used in a manner which makes them dual-use. While, to use Kaplan's (2009) words, there must be critical engagement with the potential for the services provided by Galileo and Copernicus to be applied to military purposes by users, Slijper's tone appears to suggest that he believes those programmes to be contributing directly to the militarisation of European outer space activities, which they are not. This ties in to the second problem with Slijper's assertions; that Copernicus is becoming a military asset. It is certainly possible that government users may be able to use imaging data from Copernicus for the purposes of operational planning, however Slijper's fears appear to be directed at the use of such data by European actors capable of launching military interventions abroad (2009: 35, 38). Given the logistical and manpower requirements such an action would most likely require, it is likely that actors capable of such interventions would already have access to data from military surveillance satellites, such as the French Satellite Pour l'Observation de la Terre (SPOT), which are capable of much higher flexibility and image resolution.

The distinction between EU outer space policy-making and EU Member State policy-making is quite clear when it comes to military space programmes. The national space projects of EU Member States are not restricted by the same commitment to 'peaceful' uses which constrains ESA programmes, and many states operate a range of military assets, including optical and radar remote sensing satellites providing high-resolution imagery (such as the French SPOT programme) and satellites dedicated to the transmission of military communications (an example of which is the Skynet satellites operated by the UK).

While Sheehan (2012) and Slijper (2008) may consider the shift towards the militarisation of European space efforts a fundamental contradiction with the original objectives of ESA and European collaboration on outer space affairs, taken within the context of contemporary global outer space programmes, it can be argued that Europe remains relatively pacifistic in its intentions. Although the EU appears to be favouring the use of some of its space programmes – namely Copernicus – for security applications such as border surveillance, the institution's Member States, alongside those of ESA, are displaying a reluctance to develop collaborative European systems with dedicated military capabilities. The decision to pursue an EU-managed Space Surveillance and Tracking (SST) programme was justified partly through the sentiment amongst EU and ESA Member States that ESA lacked the competence to manage military data and sensors. Meanwhile the EU is actively promoting the draft International Code of Conduct for Outer Space Activities, which includes the provision that signatories should:

> refrain from any action which brings about, directly or indirectly, damage, or destruction, of space objects unless such action is justified […] by imperative safety considerations, in particular if human life or health is at risk; or […] by the Charter of the United Nations, including the inherent right of individual or collective self-defence; or […] in order to reduce the creation of space debris; […] and, where such exceptional action is necessary, that it be undertaken in a manner so as to minimise, to the greatest extent practicable, the creation of space debris (European Union, 2013: 6).

It appears then that EU and ESA Member States are reluctant for collaborative European space programmes to include technologies dedicated to military purposes, while the EU itself is advocating stronger international agreement on avoiding the intentional destruction of objects in outer space. Although EU policies concerning outer space are becoming, and to an extent already are, militarised (see Oikonomou, 2012), the important distinction between EU military space policy and terrestrial military policies is that the former does not, for the time being, incorporate weapons programmes. Nonetheless, it is worthwhile exploring the effects that the militarisation of the EU's objectives in outer space is having upon its relationship with ESA.

2.6.1 The relationship between the EU and ESA

The architecture of European outer space activities is fairly unique, in that within Europe exist both national space agencies – such as the Italian ASI, the French Centre National d'Études Spatiales (CNES), the German Deutches Zentrum für Luft- und Raumfarht e. V. (DLR) and the UK Space Agency (UKSA) – and a regional space agency, ESA. As noted above, ESA is often assigned the role of design and procurement for pan-European outer space programmes, however Sheehan (2007) contends that:

> [a]lthough the work of ESA represents a significant contribution to the European integration process, the Agency itself is not engaged in a process of integration as such. Rather, its purpose is the *harmonisation* of European policies, so as to avoid unnecessary overlap or duplication of effort, while making possible larger-scale projects that would be beyond the resources of any single state (p. 83, original emphasis).

With regards to Galileo and Copernicus, ESA is responsible for arranging contracts with European industries for the design and construction of the satellites constituting the space segments of each programme. However, ESA's approach to the awarding of contracts to industries based upon financial contribution has been subject to criticism from the EU, which is discussed in more detail below. Nonetheless, the value of the space agency to pan-European outer space activities cannot be underestimated, as its position as a regional, rather than national, actor enables it to foster cooperation across national industries and space agencies. Unlike NASA, or even European national space agencies, ESA's competence stretches only to civilian outer space programmes (von der Dunk, 2010) and Member States of both the EU and the space agency have raised concerns over its governance of high security facilities and assets. As mentioned above, the European Space Situational Awareness (SSA) programme is a pertinent example of the tensions between civilian and military uses of outer space; the Space Situational Awareness Preparatory Programme (SSA-PP), which lasted from 2009-2012, was managed by ESA but the use of optical imaging sensors was rejected by the agency's Member States on the grounds that such sensors are capable of resolutions beyond that required for the purposes of the project (Anonymous, 2012f). In addition, upon completion of the SSA-PP, the EC announced that it, rather than ESA, would manage the development of the operational SST segment of the SSA, largely because of the need for military-operated sensors and concerns over the competency of ESA to manage highly confidential data and communications (European Commission, 2013a: 22). The civilian-military tensions over the SSA and subsequent impact upon the role of ESA in that programme are discussed in greater detail in chapter 5 of this thesis.

Although ESA may be a predominantly civilian organisation, the EU has, as discussed above, displayed an interest in exploring the potential of passive military space applications to support its terrestrial policies, and in particular the CFSP. However, the desire to militarise European space programmes necessitates a higher level of confidentiality and security than is required for civilian outer space activities. Consequently, the EC has expressed its intention to create a closer association between the EU and ESA.

In November 2012, the EC issued the Communication '*Establishing appropriate relations between the EU and the European Space Agency*'. This communication argues that the relationship between the EU and ESA is asymmetric in a number of areas revolving around funding and membership, and proposes an alternative solution of a "rapprochement" (European Commission, 2012b: 4) between the EU and ESA. The Communication suggests that this 'rapprochement' may take one of three shapes, either through:

> improved cooperation under the 'status quo', bringing ESA as an intergovernmental organisation under the authority of the European Union (following, to a certain extent, the model of the European Defence Agency), or transforming ESA into an EU agency (following the model of existing regulatory agencies) (European Commission, 2012b: 4).

Of these three alternatives, only one involves a structure where the ESA maintains it independence, although this is most likely the objective of the proposal. The EC's concern over finances is that ESA programmes are funded largely through Member State contributions on the basis that there will be some reward through the distribution of industry contracts commensurate with the contributions provided. This is at odds with the EU model, which assigns contracts based upon value and cost-effectiveness, rather than the geographical relationship between industries and countries providing funding to programmes (Spacenews.com, 2012).

The concern over membership stems from the fact that not all EU Member States are members of ESA, and conversely, Switzerland, Norway and Canada are members of ESA but not Member States of the EU. The EC argues that this is at odds with the EU's interests given that ESA decision-making is predicated upon a voting system whereby each Member State has one vote at the ESA Council, meaning that a non EU Member State could theoretically have a great influence over matters affecting the EU. In a sense, the EC desires to Europeanise ESA. However, it is clear from the Communication that the main unease of the so-called ‘asymmetric membership’ is over military and security affairs. The involvement of non-EU Member States in ESA programmes and wider ESA decision-making processes is perceived to be a potential weakness or, as the Communication puts it, an “acute problem when it comes to security and defence matters” (European Commission, 2012b: 3).

The Communication also notes the “lack [of] a structural connection and coordination mechanism within the wider policy-making of the European Union” and that “[t]he fact that ESA as a European agency has no formal link with the European Parliament deprives ESA of the direct link with citizens that any EU policy enjoys” (European Commission, 2012b: 4). These two comments are particularly revealing, as they go beyond simple displeasure with the membership and funding of ESA, pointing instead to an agenda focused upon integrating ESA within the EU governance structure. The desire to integrate ESA into the EU indicates that of the three alternatives for the future relationship between the two institutions quoted above, the first – “improved cooperation under the status quo’” (European Commission, 2012b: 4) – appears to be the least attractive to the EC.

ESA in turn responded with a resolution adopted by the space agency’s Ministerial Council on the 20th November 2012 dedicated specifically to outlining the agency’s role in European outer space activities and industry. The resolution begins with a list of ESA achievements since the last Council meeting in 2008, which, as well as summarising the developments in pan-European outer space activities between the meetings, also acts as a reminder of ESA's role in said activities (European Space Agency Ministerial Council, 2012: 4). The tone of the resolution is arguably one of defiance; a number of future challenges are named but the space agency appears to remain determined to frame these challenges and its past achievements as "[constituting] a solid basis for the full use of ESA and its assets for the benefit of Europe in an evolving and challenging context" (European Space Agency Ministerial Council, 2012: 4). As Marta (2013) observes; "ESA does not seem ready to fully accept EU rules and functioning approach and mechanisms" (p. 21).

The EU's attempts to reconfigure the relationship between it and ESA are arguably a consequence of the policy-multiplication enabled by outer space technologies. From the EC's perspective, it is not difficult to see how the efforts to promote collaborative European outer space projects may be undermined by the continued membership of non-EU states within ESA, particularly as the opportunities increase for passive military outer space applications. Should the direction of EU policy-making come into conflict with the opinions of the non-EU ESA Member States in the future, it is possible that the existing organisational architecture may well lead to further tensions between the EU and ESA.

2.6 The relationship between the terrestrial and outer space policies of the EU: European space power in action

Peoples (2010) contends that in addition to providing their own, overt purposes, European outer space technologies and infrastructures offer a subtle security advantage: they contribute directly to continued European integration, "thus preserving the political security of the Union" (p. 207; see also Peter, 2005: 266). The idea of a 'European' space stretches back hundreds of years to the religiously-unified reaches of Carolingian Christendom in the 9th Century (Jönsson *et al.*, 2000: 7). Its contemporary political reality exists through the efforts of the EU towards the 'European project', which:

> is made material by the binding power of concrete infrastructures which, it is claimed, create the potentials for movement across a unified space of flows, for an end to the fragmentation of space, and for a balancing of the forces of uneven development. The will to govern Europe, then, relies upon the idea of making a single European territory through strategies and practices of spatial intervention (Richardson, 2006: 203).

The attempts to create a single European territorial space are amalgamated by Jensen and Richardson (2004) into their theory of ‘monotopia’, which they describe as “an organised, ordered and totalised space of zero-friction seamless logistical flows” (p. 3). Such an ambition could be seen to date back to the period immediately after the end of the Second World War, when there were calls for the dissolution of European state boundaries and the establishment of a European federal state (Diez, 2006). The nation-state, which, in the eyes of the supporters of European federalism was one of the causes of the two significant global conflicts to take place in the first half of the 20th Century, was to be abolished and “superseded by common goals and a common identity” (p. 235).

While the EU may be attempting to create a seamless European space, the contentious issues involved in the process makes it far from straightforward. For example, the 2005 rejection of the proposed European Constitution was based on the contradictory criticism that it was too ‘weak’ with regards to defining its borders, yet simultaneously too ‘hard’ with regards to security and immigration (Bialasiewicz, 2008: 72).

European outer space programmes have a number of applications for European terrestrial policies, ranging from supporting border surveillance and migration, to assisting long-term studies of climate change and emergency response to environmental catastrophes (Council of the European Union, 2011). The EC Communication which proposed the ESP in April 2007 lists a series of terrestrial applications of outer space assets ranging from weather services to telecommunications, whilst commenting that "[space] can also provide valuable support to European external policies, particularly humanitarian and development policy" (European Commission, 2011b: 3). Some of the projects and applications that have been developed specifically for the Galileo and Copernicus programmes are discussed in greater detail in chapter 4, however the wider relationship between European outer space programmes and EU terrestrial policies and initiatives is analysed below. The intention here is not to provide an analysis of European space power[23] but rather to highlight the areas in which Galileo and Copernicus are supporting EU policy objectives, making them elements of policy-multiplication. Similar to force-multiplication, which refers to the use of external factors to enhance the application of force in specific circumstances, policy-multiplication involves the use of external factors by an entity to improve the effectiveness or efficiency of its policies.

After years of discussions and negotiations, the EU adopted the ESP in 2007. As well as providing much needed direction to pan-European outer space activities (see Johnson, 2006), the ESP also established the EU's role in decision-making concerning matters associated with outer space policy (Council of the European Union, 2011; Robinson, 2011b: 18). With respect to the relationship between terrestrial and extra-terrestrial policies, the Resolution on the ESP highlights the importance of outer space assets and their services to the CFSP and the EU's Sustainable Development Strategy (Council of the European Union, 2007: 3). Considered alongside the support for the Trans-European Transport Network (TEN-T) that Galileo is expected to offer, it can be argued

---

[23] A number of studies have explored growing European space power, albeit not through the lens of power projection. For instance, see Gleason (2006), Pasco (2009), Peter (2005; 2010) and Robinson (2011a).

that the EU views outer space services to be means of policy-multiplication, complementing and enhancing existing policies and projects. In a December 2011 Resolution, the Council of the European Union (2011) emphasised the “role which space systems play to provide information and practical tools for the development and implementation of European policies in the areas of environment, climate change, humanitarian aid, civil protection and crisis management” (p. 377/1). The same Resolution also recognised that:

> the completion and exploitation of [Galileo, EGNOS and Copernicus] will provide decision-makers and other users with advanced and reliable tools targeted to meet European and non-European citizens’ safety and security requirements, notably by interoperability and an integrated use of space applications for crisis management, civil protection and humanitarian assistance (p. 377/1).

Such policy-multiplication can be framed as a form of space power projection: through its main outer space programmes, namely Galileo and Copernicus, the EU is expecting to increase its internal coherence and strength, whilst simultaneously affirming its position as a noteworthy independent spacefaring actor on the international stage. In other words these programmes will, as a secondary benefit to their original purpose, assist the wider political objectives of the EU by projecting power upon users across Europe and the rest of the globe in the form of navigation and positioning services and remote sensing imagery. This projected ‘power’ is both techno-geopolitical (see Butler, 2001) and political: for Galileo, the expected proliferation of GNSS receivers designed to be interoperable with the US Global Positioning System (GPS) and Galileo will act as direct evidence of European technological might as well as a portrayal of the European programme as an equal to the US system. Moreover, as is discussed further in chapter 3, once operational Galileo will provide subscribing states with an independence from the military-operated GPS. Framing this in terms of legitimacy, the EU is arguably seeking internal and external recognition as a leader in outer space affairs through wide usage of Galileo's services and Copernicus' earth observation data. Once completed, the two collaborative projects will demonstrate the EU's capacity to develop, fund and manage significant outer space programmes distinct from the individual extra-terrestrial activities of its constituent Member States.

There is a dual astro- and geographicality at play here; the projection is originating from systems with components based both in outer space and within the Earth's atmosphere, but it is projecting upon users on Earth. In the case of Galileo, these users can access the services whilst on land, on the seas and in the air, transforming the entire globe, from the surface upwards, into a receptive area for the projection of European technological and political power. GNSS systems with global coverage offer similar space power projection, a state of affairs arguably evidenced by the near synonymy between GPS and GNSS in the minds of many users, which points to a subtle normalisation of US primacy in outer space affairs.

There is a caveat however; successful space power projection and policy-multiplication introduces dependence on the assets and technologies which enable them. In addition to acknowledging the "increasing dependence of the European economy and policies, in particular the Common Foreign and Security Policy, on space assets", the 7th Space Council resolution also notes the "critical nature of space infrastructures for autonomous European decision-making" (Council of the European Union, 2010: 9). Therefore, although the range of services originating from independent European outer space infrastructures is gradually increasing, European governments and institutions are becoming reliant on those services to maintain their “non-dependence in the current geopolitical context” (Peter, 2005: 266). The reliance on the services offered by outer space assets is not limited solely to the EU and its Member States. The US, for instance, has been warned over its dependence on outer space assets for a number of activities, from communications (United States General Accounting Office, 2002) to military operations (Joint Chiefs of Staff, 2013b: ix; Peoples, 2008: 502).

2.7 Conclusion: European collaboration and space power projection

Since the early years of ESRO and ELDO, European actors have maintained a focus on collaboration in outer space activities in order to achieve a number of long-term objectives. These objectives have largely had two common themes: contributing to independent European space capabilities and, particularly in recent years, enabling policy-multiplication using space-based technologies. These themes are not mutually independent; policy-multiplication in particular stems from wider European ambitions for independence in and leadership in a range of policy areas. The development of an independent European launcher capability has been a fundamental objective of European outer space collaboration since the 1960s, reducing European dependence on other actors whilst promoting its industrial power and scientific communities. The Galileo and Copernicus programmes, which are discussed in more detail in the next chapter, are expected to complement and enhance existing and future EU terrestrial policies on regional and external issues (Council of the European Union, 2011; European Commission, 2011b: 3). It has been argued in this chapter that they, alongside other collaborative space projects, can thus be framed as means of policy-multiplication and space power projection, contributing to the wider EU objective of seeking ‘legitimate’ leadership in outer space affairs. It can thus be argued that outer space infrastructures are integral to the EU’s ambitions both on Earth and in outer space itself.

As might be expected, the nature of activities in outer space has developed over the decades, as have the EU’s priorities for terrestrial policies. Although European collaborative efforts in outer space activities began with an explicit non-military focus, dual-use opportunities for civilian and scientific satellite systems continue to emerge. Thus it is of little surprise that the EU appears to be favouring the use of its flagship space programmes to support its regional and external policies, some of which concern security and other areas traditionally perceived as being under the blanket of military space applications. It must be emphasised however that the EU’s objectives remain relatively pacifistic, to the extent that thus far it appears determined to avoid the development of outer space technologies dedicated to military purposes. This being said, the architecture of European outer space collaboration is beginning to show the strains of competing policy objectives, and the EC Communication of November 2012 can be taken as an indication that the EU intends to increase its control over ESA operations and decision-making.

The last point of note is one of warning; although the EU and its Member States are making effective use of their outer space infrastructures, they – like others – are arguably becoming dependent upon them. These assets and the services they provide are gradually transforming into critical infrastructures requiring efforts to secure them. The next chapter will investigate the identification and security of critical infrastructures within Europe, before evaluating the extent to which the EU’s flagship Galileo and Copernicus programmes can be considered critical outer space infrastructures.

3 European critical outer space infrastructures

While infrastructures have been identified as military targets for centuries (Coward, 2009: 402), the concepts of critical infrastructures, Critical Infrastructure Protection (CIP) and Critical Infrastructure Resilience (CIR) only came to the fore in American and European political debates in the 1990s and the early 21st Century, particularly after the September 2001 terrorist attacks in the US (Burgess, 2007; Metzger, 2004: 197-198; Pursiainen, 2009: 722; Scalingi, 2007: 55). Coward (2009) argues that one of the reasons for this chronological disparity is the identification of the importance of critical infrastructures to a specific terrestrial mode of life, namely metropolitan urbanisation. While infrastructures have existed for centuries, he posits that only since the second half of the 20th Century have particular forms directly contributed to the process of 'metropolitanization' (pp. 403-404), making their protection a necessity.

As argued in chapter 2, European actors recognised from early on the need for independent launch and operational capabilities in outer space. Outer space assets can be considered tools of policy-multiplication in that they enable, complement and enhance terrestrial policies in a range of areas. In addition, independent European launch capabilities are enabling the EU to project its space-power across the Earth, as they have demonstrated European capability to launch satellites from outside the geographical constraints of Europe. However, European space power extends beyond launchers, and therefore this chapter builds upon the arguments of the previous one by focusing upon outer space assets and the infrastructures that they are part of. It begins by offering a brief history of efforts to secure critical infrastructures, from the emergence of CIP in the late

1990s to the evolution towards CIR, whereby resilience and redundancy are considered equally important to attempts to deter threats. The argument is made that instead of conceiving CIP and CIR as two separate approaches, there has been a shift within academic debates towards conceptualising CIP as part of wider CIR efforts, as protection measures are integral to wider resilience and redundancy planning. This framework is then applied to the policies of European Union (EU) pertaining to the security of European Critical Infrastructures (ECIs),[24] which are infrastructures acknowledged as being critical to more than one EU Member State. The chapter argues that satellite constellations and the services they provide fulfil the requirements to be considered critical infrastructures although they do not comply with existing regulations concerning the designation of ECIs. Finally, the two European flagship outer space programmes, Galileo and Copernicus, are outlined and framed as examples of future European critical outer space infrastructures. Some background is also provided on relevant programmes and technologies in order to locate Galileo and Copernicus within the wider context of European and international efforts to explore and exploit the domain of outer space. The chapter concludes by arguing that the future importance of the Galileo and Copernicus programmes to European societies makes their protection a matter of necessity.

As the Council of the European Union (2010) has specifically designated the Galileo and Copernicus projects to be the ‘flagship’ European space programmes (p. 4), they are the focus of this chapter looking at European critical outer space infrastructures. In addition to the economic, social and technological benefits they are expected to provide once operational, these two programmes are representative of the EU’s ambitions to

---

[24] For the purposes of this thesis, the acronym ‘ECI’ will refer only to critical infrastructures that comply with the requirements to be designated as such. The term European critical infrastructures will be used to refer to critical infrastructures owned, operated or hosted by European states regardless of compliance or non-compliance with regulations concerning ECI designation.

expand its space power through independent outer space capabilities offering services to users both inside and outside Europe. Although other operational European outer space infrastructures provide a range of critical services such as communications, remote sensing and meteorological data, the explicit acknowledgment by the EU of the importance of the Galileo and Copernicus programmes makes them ideal case studies for an analysis of their criticality.

The architecture of outer space infrastructures extends well beyond the material. There is the physical side – the ground stations, the satellites and the launch facilities – but there is also the virtual side; the connectivity which binds the material components together. As will be discussed in more detail in this and subsequent chapters, the astro-/geographical spread of the material components both on Earth and in orbit poses a challenge for conceptions of infrastructure security, while the connectivity is also problematic. Outer space infrastructures are networks; information flows between its nodes – ground stations and satellites – which have astrographical and geographical locations, albeit temporally in the case of the satellites. Both the nodes and the flow of information are critical and the disruption of either will affect the other. Therefore, when considering the security of outer space infrastructures, it is important to bear in mind both the material components (the nodes) and the connectivity (the flow of information). That being said, as outlined in the introduction this thesis focuses solely upon the security of the space segments of European critical outer space infrastructures.

3.1 Securing the vital: Critical infrastructures and the need for their protection

Before discussing in more detail the notion of ‘critical’ infrastructures, it is worthwhile briefly outlining what is meant by the term ‘infrastructure’ in the context of this thesis. ‘Infrastructure’ is very general terminology which can be loosely defined as pertaining to systems or structures which support the functioning of the state or society (see Aradau, 2010a; Coward, 2009; Metzger, 2004: 200). It thus ranges from transportation networks – such as railroads (Hartong *et al.*, 2008), motorways and bridges – to communication networks – such as satellite telecommunications, ICT networks and fibre-optic cables – and it goes without saying that some of these infrastructures will be more important – or 'critical' – to a state or society than others. It should be emphasised that infrastructures are not only the assets or structures which communicate, distribute or relay services; rather, the term comprises the entire system of assets and services. As such, infrastructure security is subject to a specific form of materiality predicated upon interconnectivity and 'intra-action' (Aradau, 2010a). In addition, infrastructures are often complex entities, constituted of a number of systems which were not originally designed to function in tandem. Egan (2007) terms these particular infrastructures Large Technical Systems (LTSs), which "will have developed through a planned, or more likely unplanned, 'rafting'[25] together of many different systems, each relying on the next for efficiency, stability and effectiveness" (p. 6). The complexity and interdependence of LTSs means that they are inherently vulnerable to failures within any part of the system (Egan, 2007: 7; see also Prieto, 2003), leading to a need for high degrees of reliability and resilience. Satellite constellations and the services they provide are pertinent examples of this 'rafting' as, they underpin many of the acknowledged terrestrial critical infrastructures. A failure in these satellite constellations could have a cascading effect upon other LTSs, leading to widespread malfunctions and failures in critical infrastructures across the globe. This is underlined by the inclusion of the Galileo programme in a pilot for the security of critical

---

[25] By 'rafting', Egan means "the joining of different elements to achieve a purpose usually unrelated to the purpose of each of the individual elements" (2007: 6).

infrastructures providing inter-state and inter-sector interdependencies within Europe (see European Commission, 2013b) discussed later in this chapter.

Efforts to secure infrastructures are, like the infrastructures themselves, often complex affairs, dealing with both the security of assets and the security of services. While assets can sometimes be protected by physical measures, such as thicker structural casing or more security personnel, the services themselves are often virtual (e.g. financial transactions) or dependent upon the existence of the assets (e.g. road networks, electrical power grids). Consequently, the two aspects of infrastructures require markedly different protection measures, which also differ depending on the specific assets and services being secured. It would, after all, be illogical to expect measures introduced to secure electrical power grids to be equally effective in protecting a state's financial system or government.

The criticality of an infrastructure is largely measured in functional terms; by the relative importance of a particular infrastructure to society and the state. Coward (2009) contends that "critical infrastructure can be said to comprise that which is constitutive of, not simply located in proximity to, contemporary metropolitan urbanity" (p. 404). In other words, critical infrastructure can be described as infrastructure which contributes to and upholds a specific form of social ordering. However, in its most abstract form, "[a] critical infrastructure is something that people depend on, either directly or indirectly, for their lives and well being [*sic*]" (Cohen, 2010: 53); in other words, critical infrastructure is fundamentally related to the survival of people, rather than social ordering.[26] Nonetheless, discourse surrounding critical infrastructure has evolved into it being seen as integral to the survival of states as well as their populations, and Clemente (2013) contends that it is "generally understood to include the particularly sensitive elements of a larger ecosystem,

---

[26] Cohen (2010) contends that the Earth and its resources of air and water are some of the most basic forms of critical infrastructure, as humankind depends on them for survival.

encompassing the public and private sectors at large" (p. 1). There is another point to be considered with regards to criticality: it is temporally contextual. As Egan (2007) notes, the extent to which an infrastructure can be considered critical "varies with the amount it is relied upon" (p. 5). To put it another way, at one moment, an infrastructure may be considered of critical importance to the state or society which it serves but this criticality is not infinite; developments – be they technological, socio-economic, political or otherwise – may occur which reduce the importance of that infrastructure to society.

In practice, states and institutions have their own definitions of critical infrastructure, although there are similarities between them. For instance, within Europe, critical infrastructure is defined by the Council of the European Union as:

> an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions (Council of the European Union, 2008a: L 345/77).

For comparison meanwhile, the US Department of Homeland Security (DHS) defines critical infrastructure as: "the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety, or any combination thereof" (United States Department of Homeland Security, 2012). The criticality of infrastructure then appears to be determined by the effect its damage or loss would have on the state in which it is based (Aradau, 2010a: 506), an understanding which Burgess (2007) describes as “necessarily *negative*” (p. 475, original emphasis), insofar as it is based upon a worst-case scenario. In this manner, the value of an infrastructure is revealed by imagining its removal from the meta-system of networks and infrastructures, highlighting interdependence and by extension, potential fragilities and vulnerabilities. However, there is a certain ambiguity on what effect the loss of an infrastructure must have in order for it to be considered ‘critical’. Whereas the US DHS definition requires a “debilitating effect” (United States Department of Homeland Security, 2012), the EU apparently perceives a “significant impact” (Council of the European Union, 2008a: L 345/77) as being worthy of an acknowledgement of criticality. The EU’s term is particularly ambiguous, as it allows the possibility that an infrastructure supporting or complementing the “vital societal functions” of a state or the “health, safety, security, economic or social well-being of people” (Council of the European Union, 2008a: L 345/77) could be considered critical, even if its failure might not prove, to employ the terminology of the US DHS, debilitating. This ambiguity, married to the focus upon Member States within the Council of the European Union’s definition, is arguably part of the process of determining responsibility for critical infrastructures in Europe, whereby it is up to individual states to identify which infrastructures they consider ‘critical’, and which they do not. It can therefore be argued that the definition of critical infrastructure has moved on from the fundamental focus of critical infrastructures as being necessary for the survival of humans and their societies, towards a focus on the survival of the state and then, by association, the safety and security of human populations. Although the safety and well-being of a state’s populace are logically an extension of state security, the focus on the political unit of the state means that infrastructures may be deemed critical despite them not primarily providing or supporting services which are crucial for the safety and security of humans.

The classification of national infrastructures as ‘critical’ is largely undertaken at the governmental level, although Dunn (2006) comments that the process is inevitably prejudiced, as “such an assessment is shaped to a large degree by subjective viewpoints and organizational backgrounds” (p. 33). Dunn also notes that the need to determine which infrastructures or sectors are deemed ‘critical’, and therefore which are not, often reverts to the mantra of ‘national security’ (p. 32). Consequently, the protection of critical infrastructures is conceived as part of a larger security problem, with the importance of those infrastructures to other networks meaning that failure to secure them threatens the security of the state. In this manner, critical infrastructures are thought of as being inherently complex entities which have emerged through the ‘rafting’ process that Egan (2007: 6) describes. In other words, their criticality is due in great part to their complex and interdependent nature. This approach has its origins in the President’s Commission on Critical Infrastructure Protection (PCCIP), which identified the protection of infrastructures as vital to national security (Dunn Cavelty, 2008: 99; President’s Commission on Critical Infrastructure Protection, 1997: vii). The PCCIP was initiated by President Clinton in 1996 and charged with assessing “the scope and nature of the vulnerabilities of, and threats to, critical infrastructures”, with the objective of recommending “a comprehensive national policy and implementation strategy for protecting critical infrastructures from physical and cyber threats and assuring their continued operation” (Clinton, 1996). However, despite the national importance of infrastructures, protection efforts following the PCCIP report – and particularly those related to cyber security – revolved around cooperation between the US government and private infrastructure owners (Dunn Cavelty, 2008). Although infrastructures may be critical at a national, or even international, level, the PCCIP decided that infrastructure owners should be responsible for the security of said infrastructures by “protecting themselves against the tools of disruption, while the government helps by collecting and disseminating the latest information about those tools and the way they are used" (Dunn Cavelty, 2008: 100). Dunn Cavelty notes though that this does not exclude the US federal government from responsibility over their own infrastructures, only those owned by private entities (p. 100).

3.2 Critical Infrastructure Protection versus Critical Infrastructure Resilience

The protection of critical infrastructures has largely been approached under the guise of CIP, which concentrates upon the protection of the infrastructure and its components (Metzger, 2004; Pursiainen, 2009). While the security of the services provided by critical infrastructures are obviously a concern, CIP advocates that the most effective method of maintaining those services is through the strengthening of the assets which carry them and the mitigation of any threats to said assets (Pursiainen, 2009).

Traditionally, within both academic literature and government reports on the protection of critical infrastructures, there has been a separation between CIP and Critical Information Infrastructure Protection (CIIP) (see Dunn, 2006; Dunn and Mauer, 2006). The threat to critical information infrastructures, has, like the need for CIP, long been recognised (see President's Commission on Critical Infrastructure Protection, 1997). Brunner and Suter (2009) present CIIP as subsidiary to CIP: "CIP comprises all of critical sectors of a nation's infrastructure, […] CIIP is only a subset of a comprehensive protection effort, as it focuses on measures to secure critical *information* infrastructure" (p. 38, original emphasis). The growth of the internet led to increasing fears amongst many security analysts of the dangers of cyber warfare (Castells, 2001: 158), while Dunn Cavelty (2008) notes that the PCCIP report commented on cyber threats more than the comparatively traditional physical dangers to critical infrastructures, although she posits that this scaremongering may well have been a means of attracting investment for new security measures (p. 99). Such was the perceived threat posed by cyber warfare, argues Scalingi (2007), that up until the terrorist attacks on the US in September 2001, CIP was understood by many in US policy-making circles to be synonymous with cyber security (p. 56).

The stark division between CIP and CIIP is not universally accepted however: Metzger (2004) warns that the "tendency to reduce CIIP (or even CI) to an issue of computer security – with its attendant focus on isolated, often technological aspects, as illustrated by terms such as 'cyber terrorism', 'cyber crime' and 'cyber warfare' – is problematic and short sighted" (p. 199). Instead, he advocates that "[i]t is the nature of the threat, not the instruments through which the threat manifests itself […], which must be taken as the basis for analysis and should serve as a guidance for institutional preparedness and defence" (p. 199). Necesal *et al*. (2011) appear to follow a similar line of thinking to Metzger (2004); while they acknowledge Information Technology (IT) as being different to other forms of infrastructure security, they argue that CIP is "complex" (p. 843) and present IT measures as another approach to security, alongside physical measures and risk and crisis management. Indeed, it is important to note though that while the focus of CIIP may be on the protection of information flowing through critical infrastructures it does not preclude some physical protection measures. The prevention of cyber-attacks on critical infrastructures, which fall under the purview of CIIP, may require some physical action, such as the installation of devices designed to secure areas or buildings from unauthorised access (Nickolov, 2005: 110). Nevertheless, the onus of CIIP is on the protection of the information which flows through the networks of critical information infrastructures, rather the infrastructures themselves.

Given the aforementioned debates over CIP and CIIP, instead of considering them as independent approaches to security there has been a shift towards conceiving them as part of a wider strategy of Critical Infrastructure Resilience (see McCarthy, 2007; Pursiainen, 2009). Both CIP and CIIP are essentially threat-based security strategies, whereby infrastructure owners attempt to accept and mitigate potential risks to their infrastructures. It is clear from Dunn Cavelty's (2008) charting of the evolution of US infrastructure protection that the early CIP rhetoric revolved around specific threats: the PCCIP (1997) report, for example, discusses a series of threats – both physical and cyber – against US critical infrastructures (pp. 14-17). Equally, during Metzger's (2004) criticism of the separation between CIP and CIIP, he refers to "the nature of the threat" (p. 199) against critical infrastructures. With a threat-based approach to the security of infrastructures, there is arguably an implicit intent to eliminate perceived threats, instead of accepting that, in the words of Pursiainen (2009): "complete protection can never be guaranteed" (p. 727; see also Aradau, 2010a: 505; Aradau *et al.*, 2008: 148). While CIP relies on a *reactive* approach to security, whereby known threats are analysed and mitigated against, CIR takes a *proactive* stance, building up protection, resilience and redundancy efforts in case of any unforeseen eventuality (Scalingi, 2007). For this reason, there has been a shift towards promoting CIR as an extension of the traditional CIP (Perelman, 2007; Pommerening, 2007: 9; Pursiainen, 2009), suggesting that infrastructure security is beginning to be considered with regards to risk-based strategies instead of threat-based ones.

CIR diverges from CIP in numerous ways but particularly in that it concentrates upon the maintenance of services, rather than only the assets providing those services (Pommerening, 2007: 15, table 1). Under the resilience approach to security, there is an acknowledgement that components of an infrastructure will inevitably fail at some point

(Garbin and Shortle, 2007: 73). Consequently, Scalingi (2007) defines a resilient infrastructure as "*a component, system, or facility that is able to withstand damage or disruption, but if affected, can be readily and cost-effectively restored*" (p. 51, original emphasis). The focus on cost-effectiveness is crucial here; as Pursiainen (2009) notes, protection is not always financially feasible, and "[a] small amount of extra protection might introduce a large amount of additional costs" (p. 727). Instead of rigid and often expensive physical protection, CIR advocates a flexible and adaptive approach to services-security, whereby aspects of a system – particularly those in a network – are designed to be capable of taking the workload of another aspect in the event of a failure. In other words: redundancy (see Garbin and Shortle, 2007: 73-74).

CIR is not limited solely to the security of specific infrastructures. Perelman (2007) takes resilient strategies beyond infrastructure, comparing US approaches to national security in the guise of 'hard' and 'soft' paradigms; he contends that the 'hard' path eventually decreases national security by inadvertently making critical infrastructures and assets 'brittle', while the 'soft' path attempts to reduce vulnerabilities in said infrastructures by "softening the brittleness of systems by reducing their vulnerability profile through redundancy, lower cost, dispersal, reduced scale, self-healing capability, accelerated repair/recovery, more 'graceful' failure modes, and so forth" (p. 28). Perelman does distance himself from CIR though, arguing that in a truly resilient society, there would be little, or no, need to identify particular infrastructures as 'critical' (p. 40). While this desire may well in the near-future apply to some areas of commerce, it is arguably unlikely that it will occur with regards to other forms of infrastructure, such as power-supply, unless there were to be a dramatic change in the way that they deliver and produce their services *en-masse*.

CIR is already in place in some countries. While commenting on European approaches to infrastructures security, Pursiainen (2009) argues that:

> [t]he Finnish approach focuses on the functions themselves rather than infrastructures that support them. The main emphasis is on the functioning of society and government in all circumstances, not only in the protection of its critical infrastructures against extreme events. Hence one could say that Finland's approach is much more based on 'resilience' […] than protection (Pursiainen, 2009: 726).

Following this line of thinking, Pursiainen later comments that the focus solely upon the protection of infrastructures, as is the case in CIP, is "becoming somewhat outdated [… and] the concept of CIP should be extended to Critical Infrastructure Resilience, of which CIP is an important part" (p. 727). It would appear that many proponents of CIR advocate such a restructuring, with one of the main concerns being CIP's focus on the protection of assets; an approach considered futile by Perelman (2007), Pommerening (2007: 18) and Pursiainen (2009: 727), amongst others. Moving towards CIR also resolves the friction discussed earlier between CIP and CIIP; there is no need for further debate about whether CIP is separate to, or inclusive of, CIIP. Instead, both constitute integral aspects of a larger CIR-based approach to security (see figure 3.1).

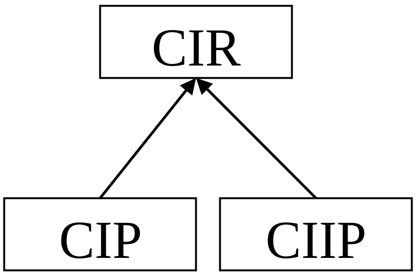

Figure 3.1 Critical Infrastructure Resilience

As Pursiainen (2009) implies, the shift from CIP to CIR does not diminish the need for asset-protection (p 727); rather, the focus on services arguably reinforces the necessity for physical and cyber infrastructures to be adequately and cost-effectively protected from known dangers. Rather than replacing CIP, CIR is an extension of the concept to encompass resilience as well as protection (Pursiainen, 2009; Perelman, 2007: 28; Pommerening, 2007); while there is no doubt that resilience allows adaptability and flexibility in the case of a crisis, balance between that and infrastructure protection must remain (see Scalingi, 2007). If anything, moving towards CIR strengthens traditional CIP, as it advocates a reduction in vulnerabilities against both known and unknown dangers, arguably making the task of protection easier. In this fashion, CIR, CIP and CIIP complement each other, enabling a comprehensive security strategy to be created and maintained at minimal cost.

The logic underpinning CIR, and to some extent CIP and CIIP, is the security of infrastructures against risks, both known and unknown. The focus on resilience and redundancy within CIR discourses is intended to ensure that even though vulnerabilities within infrastructures may have been minimised through protection measures, damage or failures to parts of an infrastructure caused by unforeseen factors or risks should not affect the entire system. It could therefore be argued that CIR measures are part of an anticipatory approach to infrastructure security, as planners and decision-makers are attempting to mitigate the impact any future risks could have upon infrastructures.

3.2.1 CIP and CIR representative of anticipatory security

Anticipatory security is an inclusive term for a number of security logics, such as preemptive or preventive security measures (Anderson, 2010), although the terminologies used differ depending on subject area (Stern and Wiener, 2006). With respect to historical inter-state conflicts, Shue and Rodin (2010a) argue that preemptive war is often associated with, and commonly justified as, an action taken to mitigate an imminent threat (p. 3). Meanwhile, Strachan (2010) suggests that preventive security measures are characteristically either actions taken by states to ensure that a potential threat does not emerge, or the engagement with a potential opponent before they are too strong. In this manner, preemptive and preventive wars are portrayed as part of a statist defensive security logic, whereby an entity attempts to deal with a threat while it is in a position of comparative strength (Stern and Wiener, 2006). The two have historically, Strachan (2010) argues, been separated by their objectives: preemptive actions have largely been small affairs, relying upon speed and precision to achieve a quick victory over a specific threat, whilst preventive action has normally taken the shape of conflicts started by states against stronger – though unprepared – powers to avoid future belligerence.

Away from the arena of inter-state conflict, anticipatory security is conceived quite differently. Instead of being used to counter imminent dangers, preemptive action “operates in the present on a future threat” (Massumi, 2007: para. 13). It is associated with the ‘precautionary principle’ (de Goede and Randalls, 2009), a term originating in environmental politics whereby “uncertainty is no excuse for inaction against serious or irreversible risks [and], that absence of evidence of risk is not evidence of absence of risk”

(Stern and Wiener, 2006: 394). The principle has been adopted by the EU in various areas of policy-making (de Goede, 2011: 6; European Commission, 2000b) and has also been applied to terrorism studies, particularly following the September 2001 attacks on the US and the subsequent global reactions (see for example Aradau and Van Munster, 2007; de Goede, 2008a, b, 2011; Stern and Wiener, 2006). The fundamental logics of the precautionary principle are the need to anticipate not only perceived threats but risks as well, and the need to adequately manage those risks.

Preventive action is conceived of as being directed at clearer dangers which can be predicted; Massumi (2007), for instance, theorises that “[p]revention operates in an objectively knowable world in which uncertainty is a function of lack of information, and in which events run a predictable, linear course from cause to effect” (para. 5). The precaution that is necessary for preemptive action is not required for preventive security measures, as these are intended to counter or mitigate a known and statistically calculable threat (de Goede, 2011: 9). Massumi goes on to argue that:

> [p]revention, in fact, has no ontology of its own because it assumes that what it must deal with has an objectively given existence prior to its own intervention. In practice, this means that its object is given to it predefined by other formations, in whose terms and on whose terrain it must then operate (2007: para. 5).

The nature of any preventive action, then, is dependent upon the risk, danger or threat it is directed upon, making it as much reactionary as it is anticipatory. It is important to note though that preventive action is still anticipatory as it is usually employed against threats or dangers which, whilst “in principle, statistically knowable and calculable according to cycles of regularity” (de Goede, 2011: 9), cannot be comprehensively defined or assessed.

The objective of anticipatory security practices is to secure against and manage future uncertainties through preemptive or preventive action. As Anderson (2010) notes, “the assumption is that the future will diverge from the past and present. It is neither a perpetuation of the present, nor an imminent-transcendent End outside of time. Instead the future will radically differ from the here and now” (p. 780). He goes on to contend that anticipatory actions are underpinned by what Grusin (2004) calls ‘premediation’, whereby the future is conceived of as a ‘surprise’ (Anderson, 2010: 782). Anderson argues that thinking of the future in this way has two consequences:

> [f]irst, disclosing the future as a surprise means that one cannot then predetermine the form of the future by offering a deterministic prediction. Instead, the future as surprise can only be rendered actionable by knowing a range of possible futures that may happen, including those that are improbable. Second, statements about the future as a surprise do not enable the future to be grasped and handled through a process of induction from the past distribution of events. Instead, anticipatory action must be based on a constant readiness to identify another possible way in which a radically different future may play out (p. 782).

Predictions of future events or risks still take place but the surprise largely pertains to the occurrence of an event, rather the event itself. Taking space weather events (SWEs) – which are discussed in detail in chapter 5 – as an example, predictions and models of the risk of a potentially catastrophic SWE on the scale of the Carrington Event[27] are on-going, as are studies of the effect that these events have on satellites and terrestrial infrastructures. The possibility that a significant SWE could occur is not in itself a surprise, however our inability to predict such an event means that there will be an element of surprise if and when one takes place. A pertinent example is the meteorite which entered the Earth's atmosphere over south-eastern Russia in February 2013, creating a shockwave which damaged buildings over a significant area and leading to a large number of injuries amongst people living in the area. In addition, there is always the chance that an unforeseen danger could emerge, providing both surprise at the event and surprise at the occurrence.

Both preventive and preemptive anticipatory security practices are intended to compensate for and mitigate future surprise, the difference between the two being that the former act upon 'known' threats or hazards – ones with an "objectively given existence" (Massumi, 2007: para. 5) – whilst preemptive measures are directed towards uncertain future risks. The element of 'knowledge' is crucial; de Goede (2011) contends that prevention is commonly associated with "risks that are, in principle, statistically knowable and calculable according to cycles of regularity" (p. 9). In other words, historical data and statistics are used to calculate the probability of events occurring again in the future. Preemption meanwhile "addresses threats, risks and dangers that are irregular, incalculable, and, in important ways, unpredictable" (de Goede, 2011: 9). In terms of the risks and dangers to the space segments of outer space infrastructures, the existing space debris population and most space weather phenomena could arguably be classified as "statistically knowable and calculable [risks] according to cycles of regularity" (de Goede,

---

[27] The Carrington Event of 1859 remains the largest SWE on record. See chapter 5 for further discussion of the Carrington Event and associated studies of large-scale SWEs.

2011: 9); efforts to track and catalogue the existing debris population and the scientific monitoring of solar activity are directed at ensuring that it is possible to calculate the probability that these risks may threaten outer space infrastructures. However, future debris generation and significant space weather events constitute dangers for which precaution is necessary given that they are impossible to predict or their effect upon outer space infrastructures is uncertain.

Nonetheless, the three-dimensional spatio-temporal nature of geocentric orbits means that although some phenomena such as the existing space debris population are ‘known’, the danger they pose to satellites is not always clear. A hypothetical piece of catalogued space debris – the existence, size and orbital trajectory of which are known – may not pose a threat to other space objects in its current orbit, but if its trajectory were to be altered in any way – for instance through atmospheric drag – it may become a collision risk for nearby satellites. Equally, unannounced or unexpected manoeuvres by operational satellites can expose other space objects to the possibility of collision that did not exist before. Anticipatory security practices oriented towards outer space activities must therefore account not only for the generic danger posed by threats – the capacity for phenomena to cause damage to satellites and other space objects – but also the likelihood that specific satellites or other space objects will be exposed to those threats. Consequently, the outer space environment arguably challenges Massumi’s conception of prevention, as measures directed at ‘known’ dangers – such as the existing space debris population – must still take into account the element of ‘surprise’ rather than expecting “events [to] run a predictable, linear course from cause to effect” (Massumi, 2007: para. 5).

For the sake of clarity, it is worth emphasising that anticipatory security practices occur after an entity has identified which risks and dangers they consider threatening. The identification act itself has no effect upon the risks and dangers themselves, as it simply represents the prioritisation of certain threats over others. Nonetheless, the predictability of the risks and dangers – be they “statistically knowable and calculable according to cycles of regularity” (de Goede, 2011: 9) or “irregular, incalculable, and, in important ways, unpredictable” (de Goede, 2011: 9) – may well influence whether or not they are deemed threatening. To put it another way, it is possible that entities may perceive calculable and predictable risks as more urgent and threatening than unpredictable ones, even if the latter’s potential impact is greater.

The security of critical infrastructures, particularly through CIR though to some extent through practices associated with CIP, are also geared towards uncertain or unknown risks and dangers, although logics of anticipatory security are arguably understudied in literatures concerned with these approaches to infrastructure security. However, significant investment is required for some of these infrastructure security practices, meaning that they could be considered risks themselves. Simulations, such as war games (Der Derian, 2009b), digital simulations in aviation (Budd and Adey, 2009) and preparedness exercises (Adey and Anderson, 2012; Aradau, 2010b), can be quite costly and time-consuming and the scenarios played out may never materialise. Their function is to limit future surprise by conditioning those involved to possible future events, to the extent that the scenarios may remain ingrained in the minds of those who participated and in recorded in digital or written reports, existing in a state of uncertainty between the real and the imagined/virtual. The events have ‘taken place’, insofar as participants have been faced with choices, reacted to them and had to deal the consequences, even if only in their imagination. Although those involved may not have experienced the full extent of the scenarios as they would have done if they had been ‘real’, the objective of simulations, war games and exercises is nonetheless to simulate events in a manner that is as close to reality as is considered feasible by the organisers, or as far as the suspension of disbelief will allow (Adey and Anderson, 2012: 100). This conditioning, although serving to improve the resilience of participants in the face of an unexpected or overwhelming event, may well blur the margins between the probable and improbable, or even the real and the simulated (Der Derian, 2009b). Nonetheless, the objective of these practices is to instil a sense of preparedness within those participating, so that if, or when, faced with a similar scenario, they will be capable of reacting based upon an experience, simulated though it may be. As Aradau (2010b) notes with respect to preparedness:

> [p]reparedness does not try to find a rational way to avoid the 'next terrorist attack' or to confront it with superior knowledge, but to use artifice to avoid its consequences and ensure the self-preservation of atomistic individuals, the entrepreneurs who have taken precautionary measures. Artifice allows exercise players, like Odysseus, to lose themselves in order to save themselves (p. 4).

Other forms of CIP and CIR measures can be considered risky due to the sizeable investment required. As mentioned earlier, the physical protection of assets or hardware can in some cases add considerable expenses to the development, construction or deployment of the assets themselves (Pursiainen, 2009: 727). With regards to space assets, for instance, any increase in weight requires more fuel or, depending on the amount of weight added, even a larger launch vehicle. The cost-effectiveness of such anticipatory measures against the risk of collision with space debris is thus an important consideration for satellite designers, and will be discussed in more detail in chapter 5, however it should be emphasised that the cost-effectiveness factor makes the measure itself an exercise in risk-management. In other words, satellite manufacturers and the institutions or states which order the satellites are having to constantly assess whether the physical protection of a satellite against a particular danger is worthy of the additional costs that protection might create, or whether the danger itself can be mitigated through other means, such as increased awareness of the near-Earth orbital environment or a stronger system of governance for outer space activities.

The need to strike a balance between the security of infrastructures and cost-effectiveness means that CIP and wider CIR practices can indicate what future events a state or institution considers more probable than others, as well as the overarching approach that state or institution has to its security. To take the example of the risk that near-Earth orbital space may in the future be host to active weapons systems; the actions of states around the globe have varied from undertaking further research into orbital weapons platforms, to engaging more with legal instruments aimed at minimising the likelihood of such platforms being deployed. The weaponisation issue is a very complex one and will be discussed greater detail later, however the summation above is nonetheless indicative of the different approaches that may be taken to a particular problem. Chapters 4 and 5 of this thesis focus upon the practices and measures aimed at mitigating risks and dangers against European critical outer space infrastructures, and the specific visions of the future these imply. However, it is first necessary to provide some background of terrestrial European critical infrastructures and of the steps the EU has taken to acknowledge its satellite constellations as being critical infrastructures themselves.

3.3 European Critical Infrastructures

In the aftermath of the terrorist attacks in the US on the 9th September 2001, the protection of ECIs was allocated to the North Atlantic Treaty Organisation (NATO) (Pursiainen, 2009: 723). However, Pursiainen (2009) argues that by 2005, there had been another shift in responsibility towards the EU (p. 724). Indeed, the European Commission (EC) published the *Communication from the Commission on a European Programme for Critical Infrastructure Protection* in 2006, in which plans are outlined for, as the name of the document suggests, a European Programme for Critical Infrastructure Protection (EPCIP). This followed a Communication from the EC a year earlier relating specifically to the security of European critical infrastructures from terrorism (see European Commission, 2004). Although acknowledgement of critical infrastructures' importance began later in Europe than in the US (Pursiainen, 2009: 722), there has since been considerable debate over means of identifying and protecting them. On the identification of ECIs, the Communication states that they:

> constitute those designated critical infrastructures which are of the highest importance for the Community and which if disrupted or destroyed would affect two or more MS, or a single Member State if the critical infrastructure is located in another Member State (European Commission, 2006a: 4).

This definition has been further refined in the 'Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection', which establishes that:

> 'European critical infrastructure' or 'ECI' means critical infrastructure located in Member States the disruption or destruction of which would have a significant impact on at least two Member States. The significance of the impact shall be assessed in terms of cross-cutting criteria. This includes

> effects resulting from cross-sector dependencies on other types of infrastructure (Council of the European Union, 2008a: L 345/77).

It would appear then that there are two levels of critical infrastructure within the EU; the first of which pertains to infrastructures deemed critical by national governments, and the second which includes infrastructures deemed critical by the EC. Crucially, the 2008 Directive clarifies that ECIs must now ‘significantly impact’ two separate Member States, implying that infrastructure may only be considered critical on the European level if more than one state is dependent upon it. The removal of the statement “or a single Member State if the critical infrastructure is located in another Member State” (European Commission, 2006a: 4) from the definition contained within the 2006 *Communication from the Commission on a European Programme for Critical Infrastructure Protection* suggests that a hypothetical situation, whereby a Member State is dependent on infrastructure located in another Member State, despite the second state not deeming said infrastructure ‘critical’, is no longer feasible.

Importantly, the identification and classification of infrastructures as ECIs takes place at state level. Member States wishing to designate particular infrastructures within their borders as ECIs are required by Article 4 of Council Directive 2008/114/EC to inform other Member States dependent upon those infrastructures about their intentions. Bilateral or multilateral negotiations will then take place between all “significantly affected” (Council of the European Union, 2008a: L 345/77) parties with the intention of agreeing to classify an infrastructure as an ECI, though the identity of any ECI shall remain confidential only to the Member States affected. In the case that a Member State feels an infrastructure located within the territory of another state should be designated an ECI, it should contact the EC, which will initiate bilateral or multilateral negotiations with all affected parties (Council of the European Union, 2008a: L 345/78).

The final point to be considered from the Council of the European Union's definition of ECIs is the requirement that any candidate infrastructure must be "located in Member States" (Council of the European Union, 2008a: L 345/77). While this geographical requirement is relatively ambiguous, the argument can be made that it implies that the entirety of a critical infrastructure must be located within the territorial boundaries of Member States in order for it to be categorised as an ECI. This logically means that outer space infrastructures, the subject of this thesis and discussed in greater detail later in this chapter, are not eligible for the label 'European Critical Infrastructure'. Not only are the space segments of such infrastructures based beyond the confines of the Earth's atmosphere, but many of the ground segments (e.g. relay stations and launch sites) are located across the globe (Anonymous, 2012b). Although the Arianespace launch facility in Kourou, French Guiana, is located within an overseas department of France, the use of Russian launch sites and the spread of relay stations and ground control segments across EU and non-EU Member States is at odds with article 2(b) of Council Directive 2008/114/EC (see Council of the European Union, 2008a: L 345/77). Moreover, the European Geostationary Navigation Overlay System (EGNOS) and Galileo programmes are described the European Parliament and the Council of the European Union (2013) as "infrastructures set up as trans-European networks of which the use extends well beyond the national boundaries of the Member States" (p. L 347/1). This is problematic as it means that European outer space infrastructures, which provide vital services supporting a host of terrestrial critical infrastructures, are not themselves identified as being considered 'European' critical infrastructures merely because of their multiple astro- and geographical locations. It is possible that an exception to this geographical restriction has been made for outer space infrastructures, however bearing in mind that the identity of ECIs must remain confidential, it is highly unlikely that a public acknowledgement of any such exception will materialise.

The relationship between the geographical location of critical infrastructures and their eligibility for ECI status is arguably problematic, not only for outer space infrastructures but for terrestrial ones as well. As discussed earlier in this chapter, infrastructures extend beyond the material assets and hardware which are often their most visible aspects. The connectivity within and between infrastructures is also extremely important and can exist physically, in the shape of pipelines for gas and oil, or virtually, through the flow of digital information across cyber networks. With regards to outer space infrastructures, this connectivity is largely virtual but plays a vital role in the functioning of the infrastructure and is arguably as important as the material assets it links. If the connection is lost between satellites, or between them and their ground control segments, then the assets themselves are rendered redundant, even though they may be still be operational. Moreover, the connectivity is not impervious to astro- and geographical obstacles: the various radio-communications which enable extra-terrestrial operations require line of sight between receivers on satellites and terrestrial ground stations. In addition, launch facilities are also integral to the connectivity of an outer space infrastructure as they enable the deployment of material assets into orbit, which is of vital importance in the development of an infrastructure or the event of a satellite failure. As noted in chapter 2 of this thesis, ESA has one launch facility operated by Arianespace and located in Korou, French Guiana. Meanwhile, Galileo’s ground segment includes control stations, survey stations, upload stations, and Search and Rescue (SAR) data collection stations spread across the globe (European Commission, 2012a: L 52/30-L 52/31). Therefore, tying down an infrastructure to a specific geographical location or container –

such as the state – ignores the connectivity necessary for infrastructures to perform the tasks for which they are designed and presents a simplified perspective of the complex networks and vulnerabilities upon which they are founded.

The aforementioned issues pertaining to the narrow definition of ECIs have seemingly not gone unnoticed. In 2013, the EC published a Commission Staff Working Document exploring means of improving the EPCIP. The Working Document notes that "less [*sic*] than 20 European critical infrastructures have been designated" and that "[s]ome clear critical infrastructures of European dimension, such as main energy transmission networks, are not included" (European Commission, 2013b: 4). Indeed, the EC is of the opinion that "[d]espite having helped foster European cooperation in the CIP process, the [EPCIP] Directive has mainly encouraged bilateral engagement of Member States instead of a real European forum for cooperation" (p. 4). The need for increased cooperation between EU Member States and states outside the EU is also emphasised (pp. 5-6). The answer proposed in the Working Document is a shift away from the existing "sectoral approach, where each sector is treated separately with its own risk methodologies and risk ranking", towards a "systems approach, where critical infrastructures are treated as an interconnected network" (p. 7). In addition to introducing new forms of risk associated with interdependency, this shift is arguably reflective of the arguments made by Aradau (2010a) on the need for awareness of the materialities of interconnectivity and intra-action, as well as Egan's (2007) work on LTSs. The pilot programme for this new approach to the EPCIP involves four critical infrastructures: "Eurocontrol, Galileo, the electricity transmission grid and the gas transmission network" (p. 7). One of the reasons given for the selection of these four infrastructures for this pilot is the inherent interdependencies involved:

> [t]hey are cross-border both physically (i.e. the infrastructures are located in the territory of more than one Member State) and at the level of the service provided (i.e. a disruption of service in one Member State can affect several other Member States – a domino effect) (p. 7).

It must be emphasised that this pilot programme is in its early stages, with a report on progress due to be made in late 2014 (European Commission, 2013b: 10) but nonetheless, the recognition of inter-state interdependences upon critical infrastructures can be seen as a positive step towards addressing some of the problems with the current ECI-designation process.

Returning to the security of ECIs, the EC maintains in the 2006 *Communication from the Commission on a European Programme for Critical Infrastructure Protection* that it:

> will avoid duplicating existing efforts, whether at EU, national or regional level, where these have proven to be effective in protecting critical infrastructure. EPCIP will therefore complement and build on existing sectoral measures (European Commission, 2006a: 3).

No further information is given in that particular document, however, about how it will be decided whether existing protection efforts are ‘effective’ enough to be left in the hands of national governments, although paragraph 14 of Council Directive 2008/114/EC states that this process will rely upon cooperation between Member States and the EC:

> Each Member State should collect information concerning ECIs located within its territory. The Commission should receive generic information from the Member States concerning risks, threats and vulnerabilities in sectors where ECIs were identified, including where relevant information on possible improvements in the ECIs and cross-sector dependencies, which could be the basis for the development of specific proposals by the Commission on improving the protection of ECIs, where necessary (Council of the European Union, 2008a: L 345/76).

Importantly, paragraph 6 of the Directive states that "[t]he primary and ultimate responsibility for protecting ECIs falls on the Member States and the owners/operators of such infrastructures" (Council of the European Union, 2008a: L 345/76), suggesting that despite the regional importance of ECIs, protection will still take place primarily at national level, with European 'Community level' action being employed to complement existing protection measures (p. 2). However, there appears to be little regulation of what measures should be implemented by Member States to address security issues (Necesal *et al*., 2011: 843).

While the aforementioned Council Directive is aimed specifically at the protection of ECIs within the energy and transportation sectors, it "constitutes a first step in a step-by-step approach to identify and designate ECIs and assess the need to improve their protection" (Council of the European Union, 2008a: L 345/77) and thus can be considered representative of the EU's approach to the overall protection of ECIs.

As discussed earlier, while protection is a significant part of CIP, it represents only one particular aspect of CIR. Although resilience is not specifically mentioned in EU policy documents with regards to ECIs, it is alluded to in a manner suggesting that is understood to be within the process of CIP; the 2006 *Communication from the Commission on a European Programme for Critical Infrastructure Protection* states that "[c]ontingency planning is a key element of the CIP process so as to minimize the potential effects of a disruption or destruction of a critical infrastructure" (European Commission, 2006a: 8). Given that contingency is a crucial aspect of resilience (see Scalingi, 2007), it can be concluded that some form of resilient strategy is at the forefront of European policy-making, albeit under the guise of CIP.

It appears though that the EU has not completely adopted the resilience-based approach to security. The 2008 Council Directive 2008/114/EC defines 'protection' as: "all activities aimed at ensuring the functionality, continuity and integrity of critical infrastructures in order to deter, mitigate and neutralise a threat, risk or vulnerability" (Council of the European Union, 2008a: L 345/77). On the one hand, the definition implies some form of resilience given the inclusion of the terms 'continuity', 'risk and 'vulnerability', however the desire to "deter, mitigate and neutralise a threat, risk or vulnerability" (p. L 345/77) arguably hints at emphasis upon a more traditional and reactive approach to CIP. As mentioned earlier, the intent to eradicate threats or vulnerabilities is commonly agreed within resilience literature to be impossible, hence the need for contingency in the event that prevention and protection efforts fail.

Notably, the introduction to a 2013 EC Staff Working Document states that "[b]y **ensuring a high degree of protection of EU infrastructures** and **increasing their resilience** (against all threats and hazards), we can minimise the consequences of loss of services to society as a whole" (European Commission, 2013b: 2, original emphasis). While protection remains prominent, the explicit reference to need for resilience can be seen as an acknowledgement of the vulnerability of critical infrastructures and the impossibility of complete protection. Although the Staff Working Document is only a proposal describing a pilot programme, it is nonetheless indicative of a shift in EU policy-making with respect to the security of critical infrastructures upon which European societies depend, albeit one which has not been formalised at the time of writing.

3.4 CIP, CIR and European security in outer space

Regarding the security of European outer space assets and the services they provide, there appears to be little reference to their designation as critical infrastructures until relatively recently.[28] The shift notably came to light with a speech by the President of the EC in 2009, who stated that "we need more security in and from space. Our space assets and infrastructure are indispensable for our economy and security and we need to protect them" (Barroso, 2009: 3). Although the 2007 *Communication from the Commission to the Council and European Parliament European Space Policy*, states that "[s]pace-based systems […] are critical to key areas of the economy" (European Commission, 2007b: 3), the explicit designation of outer space assets as segments of critical infrastructures in need of security does not appear to have been made public prior to President Barroso's 2009 speech. This stance is continued in the EC *Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions towards a space strategy for the European Union that benefits its citizens*, which proposes that:

> [s]pace infrastructure is critical infrastructure on which services that are essential to the smooth running of our societies and economies and to our citizens' security depend. It must be protected and that protection is a major

---

[28] Although an EC Communication concerning Galileo mentions the security of infrastructures, it identifies these as "control centres and communication networks" and does not mention the outer space assets themselves (European Commission, 1999: 11).

> issue for the EU which goes far beyond the individual interests of the satellite owners (European Commission, 2011a: 6).

Three details from this quote stand out. The first is the identification of outer space infrastructure as ‘critical infrastructure’, which is indicative of its perceived importance to European societies in general. This association between the terrestrial and the extra-terrestrial is a microcosm of the EU’s wider involvement in outer space affairs, whereby the institution has gradually recognised the importance of space assets to modes of life on Earth (see Sheehan, 2011: 45; chapter 2 of this thesis). Importantly, there is no identification of specific infrastructure within the aforementioned Communication; rather, all outer space infrastructures are considered ‘critical’, an issue discussed further below. While this may have been done to avoid the targeting of specific outer space systems, it is nevertheless telling of the dependence terrestrial societies now have on extra-terrestrial infrastructures. Nonetheless, the reference to ‘satellite owners’ is indicative of an implicit acknowledgment of the need to secure Earth-orbiting assets as well as the services they provide. In addition, in the 7th Space Council resolution, the Council of the European Union calls upon “the EU, ESA and their Member States to undertake the necessary actions […] to protect satellites and satellite signals and to secure frequencies, taking into account emerging new threats to space assets” (Council of the European Union, 2010: 3-4). This paragraph reveals the objects recognised as requiring protection measures, essentially identifying what the EU perceives as the integral aspects of its outer space infrastructures. The 8th Space Council resolution follows this line of thinking, stating explicitly that outer space infrastructures are “critical” (Council of the European Union, 2011: C 377/1) but, as might be expected, goes into more detail. Notably, the ground segments of outer space infrastructures are included alongside outer space assets as being vulnerable to certain threats (Council of the European Union, 2011: C 377/4), but there is no mention of space or ground segments being targeted by state or non-state entities to disrupt the flow of satellite services. Two risks are explicitly acknowledged within the 8th Space Council resolution: collision between space objects and space weather events, although there is an implicit nod to human activities in outer space in paragraph 29 of the resolution. That paragraph notes, with reference to the draft International Code of Conduct for Outer Space Activities, that "wider access to adequate and reliable information about space activities will represent a confidence building measure, providing a foundation for increased trust with regard to peaceful uses of outer space" (Council of the European Union, 2011: C 377/4).

The sentence used by the European Commission – "[s]pace infrastructure is critical infrastructure on which services that are essential to the smooth running of our societies and economies and to our citizens' security depend" (European Commission, 2011a: 6) – can arguably be interpreted in two ways; either that all space infrastructures are critical infrastructures or that only outer space assets providing critical services can be deemed to be outer space infrastructures. Both of these understandings are arguably problematic. Beginning with the first interpretation, that all outer space infrastructures are 'critical' (see European Commission, 2011a: 6), there is the issue that while some satellite systems may well contribute to and uphold the contemporary mode of life on Earth, not all of them do. For similar reasons to Wang (2009), when he dismisses scientific outer space programmes from his analysis of transatlantic astropolitics (p. 435), it could be argued that the loss of some satellites, while costly and to the detriment of scientific study, would in all likelihood not severely affect terrestrial societies in the same way that the loss of Global Navigation Satellite Service (GNSS) signals, for example, would. While it could be assumed that there are valid reasons behind the blanket imposition of criticality, such as obscuring the identification of those systems and networks which are truly valuable, at first glance an interpretation labelling all outer space infrastructures as ‘critical’ hints at a European hesitation and uncertainty regarding the focus of outer space security efforts. The second understanding of the above quote, that only outer space assets providing critical services can be designated as outer space infrastructures, is equally problematic. Although it does avert the blanket imposition of criticality of the first interpretation, all outer space assets, including scientific missions not integral to the “smooth running of […] societies and economies and to […] citizens’ security” (European Commission, 2011a: 6) arguably comply with the definition of infrastructure used at the beginning of this chapter (see Aradau, 2010a; Coward, 2009; Metzger, 2004: 200). To put it another way, all outer space assets contribute to the functioning of the state or society, even if the disruption of their services would in all likelihood not cause problems significant enough for those services to be deemed critical. Consequently, all outer space assets and their respective ground segments are arguably outer space infrastructures. Given the problems associated with both interpretations of the quote from the 2011 EC Communication, the argument can be made that the EC’s definition of outer space infrastructures is too ambiguous and requires clarification. Moreover, the 2013 European Commission Staff Working Document introducing a pilot programme regarding the security of inter- and intra-sectoral interdependencies states that:

> [s]pace-based systems enable a wide spectrum of applications, which play a fundamental role in our everyday life, are critical to key areas of the economy, and help ensuring our security. […] the ability to protect space infrastructure has become essential to our society (European Commission, 2013b: 13).

While this would appear to support the first interpretation of the quote from the 2011 EC Communication, issues remain concerning the blanket imposition of criticality upon services which are not necessarily critical. Nonetheless, despite the issues outlined above these definitions cannot simply be ignored. By seemingly attributing criticality to all outer space infrastructures, the EC is arguably implying that all services provided by outer space assets need to be secured. The second detail of note from the EC Communication is that outer space infrastructure "[m]ust be protected" (European Commission, 2011a: 6). Unfortunately, little more detail is provided within the aforementioned Communication about what form(s) of protection exists regarding space infrastructure. There is however an acknowledgment of the need for a European Space Situational Awareness (SSA) system to enhance monitoring capabilities of potential dangers and threats to active satellites (European Commission, 2011a: 7; European Commission and European Space Agency, 2010: 3-4), a need which echoes Barroso's (2009) call for "an independent capacity to monitor satellites and debris orbiting the Earth and space environment, and tackle possible hazards" (p. 3). The SSA arguably represents part of an extra-terrestrial CIP approach conforming to the EU's territorial CIP strategy, as the intention is, in the words of Council Directive 2008/114/EC on European critical infrastructures, to "mitigate and neutralise […any] threat, risk or vulnerability" (Council of the European Union, 2008a: L 345/77). The importance of the SSA to the security of European outer space infrastructures is re-iterated in the 8th Space Council resolution, which foresees an "effective" SSA as having the capability to "enhance the safety of European space assets and of its future launches from space debris and other objects in outer space as well as space weather phenomena" (Council of the European Union, 2011: C 377/4). Nevertheless, combined with the reference to resilience in the 2013 EC Staff Working Document (European Commission, 2013b: 2), the explicit recognition of the need to protect outer space infrastructures as well as the services they carry and provide marks a positive shift in the European strategy for outer space security.

The distinct absence of information in EU publications pertaining to the means undertaken to ensure the security of European outer space infrastructures could be explained by the requirements of Council Directive 2008/114/EC. By describing outer space infrastructure as ‘critical’, the EC has associated it with terrestrial critical infrastructure, meaning that their protection falls under the purview of Council Directive 2008/114/EC, which includes the provision that information regarding the protection of ECIs is classified as confidential (Council of the European Union, 2008a). It is thus possible that details or summaries of protection or resilience measures for outer space infrastructures cannot be publicly disseminated. Nonetheless, it is noteworthy that while European outer space infrastructures have been categorised as critical infrastructures by the EC, this classification does not appear to have been translated into wider CIP or CIR discourses on ECIs.

The final detail of interest from the quote from the EC Communication pertains to the role space infrastructures play in European societies. Specifically, the Communication states that “[s]pace infrastructure is critical infrastructure on which services that are essential to the smooth running of our societies and economies and to our citizens’ security depend” (European Commission, 2011a: 6). The breadth of terrestrial critical infrastructures was mentioned earlier in this chapter, however many, if not all, of these infrastructures rely on services provided partially or entirely through satellites. To offer two examples; the provision of food and other essential goods to populations relies upon GNSS signals to enhance the efficiency of the transportation of those goods through the skies, by road and by train. Equally, the contemporary financial system depends upon the precise timings transmitted by the atomic clocks present within GNSSs. Should these timings lose synchronisation or cease to be transmitted, it is entirely possible that regional, or even global, financial transactions could be affected. It could therefore be argued, using the aforementioned quote as supporting evidence, that outer space infrastructures underpin the majority of other critical infrastructures, making them not only part of the ‘rafting’ process described by Egan (2007) but also particularly essential to European societies.

As each satellite or satellite constellation has different properties and functions, they operate at differing altitudes above the Earth. Consequently, the risks which must be considered when planning their security vary; for instance, satellites orbiting in lower orbits need not be provided with as robust radiation shielding as satellites in MEO, which are located at the heart of the Van Allen radiation belts. It should also be noted that there is often redundancy and resilience included within satellite constellations providing critical services, such as the US Global Positioning System (GPS), so that if one satellite should malfunction or be interfered with, a reserve satellite can be used to minimise the impact on the transmission of signals. As this thesis is taking for case studies the Galileo and Copernicus projects, the security measures it will examine will be mainly limited to those applicable to satellites in LEO and MEO, although some issues, such as frequency and orbit slot allocation, will be discussed as part of the wider outer space security problem.

3.5 Galileo

The drafting of the Convention of the European Launcher Development Organisation (ELDO) in November 1961 signalled the beginning of efforts to construct an independent European launcher capable of putting satellites into outer space (Madders and Thiebaut, 1992: 117; Sheehan, 2007: 77). As mentioned in chapter 2, one of the most significant factors in the establishment of ELDO was the scientific and political collaboration which emerged through the development of the Europa launcher, even though the project was eventually abandoned in the 1970s.

The failure of the Europa launcher, while a setback for European outer space affairs, does not detract from the project's reflection of the desire amongst European states to develop an independent outer space capability. In 1976, the ESA Director of Planning and Future Programmes described the sought-after European independence in outer space affairs thusly: "[i]ndependence here does not mean isolation or refusal to co-operate, but refusal to accept uncontrolled dependence" (Lebeau, 1976: 3). This desire was, and still is, present in the motivations behind the Galileo project (see European Commission, 1999); while the US GPS addresses many, if not most, European needs, the US reserves the right to deny access to its signals in times of war. The absence of a guaranteed service means that any systems that rely on GPS signals could potentially be crippled in the occasion, however unlikely it may be, that the US were to withhold access to those signals. As Sheehan (2007) contends, such concerns "triggered a similar response to the move into launcher technology in the 1960s. It was not enough to have guaranteed access to US capabilities virtually all the time, Europe needed a system under its own control that it would have access to on a permanent basis" (p. 88).

On the 10th February 1999, the EC issued a Communication calling for the establishment of an independent European GNSS, named Galileo, to reduce European dependence on GPS and the Russian Globalnaya Navigatsionnaya Sputnikovaya Sistema (GLONASS). The programme was approved by the European Council in June 1999 at a meeting in Cologne (Bolton, 2012: 192), making it the first joint EU/ESA project (European Space Agency Director General, 2003: 5). The importance of GNSS services to European civil and military interests was clear to the EC and the risk of losing access to those services through a potential denial of access by the US was a great strategic concern

(European Commission, 1999: 2). It was made clear from the outset that Galileo would address weaknesses of GPS and GLONASS, particularly in terms of accuracy and reliability (European Commission, 1999: 2), while maintaining a purely civilian approach (Martin *et al.*, 2009: 3). In particular, the EC was concerned that "[t]here are serious problems of sovereignty and security if Europe's critical navigation systems are out of Europe's control. Furthermore, the present system cannot fully meet civil users [*sic*] requirements in terms of performance" (European Commission, 1999: iv).[29] The civilian nature of the project was in itself a novel concept, as both GPS and GLONASS are operated by their respective state's military (Elhefnawy, 2003: 57; Martin *et al.*, 2009: 3).

In 1999, GPS and GLONASS dominated the GNSS market (European Commission, 1999: 2), though investment in GLONASS stalled following the collapse of the Soviet Union (Bolton, 2012: 192), to the extent that only eight satellites, out of a constellation of 24, were operational in 2000 (Mathieu, 2010: 357) and GPS became the superior system. A GNSS uses precise timing and geometric triangulation to offer accurate three-dimensional positioning to users (Lindström and Gasparini, 2003: 6) and consequently has a myriad of applications, including, but not limited to, improving accurate navigation, efficient transportation, energy distribution and banking (European Commission, 2006b: 3-4). The 1999 EC Communication estimated that the market for GNSS applications would be in the whereabouts of €40 billion by 2005 (European Commission, 1999: 3), while a 2006 Green Paper estimated that this figure would rise to €400 billion by 2025 (European Commission, 2006b: 2). In 2007, it was suggested that exploitation revenues from the Galileo programme could range between €4.6 and €11.7 billion over a 20 year period (European Commission, 2007c: 6).

---

[29] The applications of Galileo and the role they play in supporting the European project will be the subject of further discussion later in this chapter.

The European fears that access to GPS could be denied were not without foundation. This is evidenced by the system's signal architecture, whereby the civilian and military signals transmitted by GPS are independent of each other. The civilian Coarse/Acquisition (C/A) Code only uses the L1 frequency while the military Precision Code (P-Code) uses both the L1 and L2 frequencies, increasing its accuracy and reliability (Bolton, 2012: 191). However, this means that the C/A Code can be jammed without significantly affecting the P-Code (Blanchard, 2003). The next generation of GPS satellites, GPS III, will include an updated and more robust military signal, called the M-Code, along with an improved civilian signal (Globalsecurity.org, 2011b), though the capability to deny access to the civilian frequencies will remain.

Although the EC called for reduced dependency in its February 1999 Communication, it was not intending to construct a new GNSS on its own; negotiations took place in 1998 with the US over a possible collaborative project, but the offer was turned down by the US on military grounds. This did not deter the EC however, and from the outset there were plans to include non-European states within the project, including Russia and Japan (Europa.eu, 2006), while interoperability between Galileo and GPS was considered of great importance (European Commission, 1999: 8-9). The 2007 European Space Policy (ESP) continues this trend, noting positively that "[m]any non-EU countries are seeking to become partners in the programme" (European Commission, 2007c: 5). In 2003, an agreement was met between the EU and China over a Chinese investment of around €200 million into the Galileo programme in return for a 20% share of the project (Wang, 2009: 451-452), although access to the Public Regulated Service (PRS) was not discussed (Bolton, 2012: 195).[30] From these events, it could be concluded that while the

---

[30] Collaboration between the EU and China over the Galileo programme effectively ended in 2010 following the announcement that Chinese payloads would be removed from the four initial satellites (de Selding, 2010).

EU is trying to consolidate its European spatial integration and independence through its outer space programmes, it is simultaneously acknowledging the importance of external investment and its inability to fund such ventures on its own.

The 1999 Communication was followed up by an EC Communication in 2000 whereby a development plan for Galileo was established. This plan called for a development and validation phase, to last between 2001 and 2005, a deployment phase between 2006 and 2007 and, finally, an operating phase from 2008 onwards (European Commission, 2000a: 6). However, technical and financial obstacles severely delayed the project, to the extent that the first Galileo In-Orbit Validation Element (GIOVE) satellite, GIOVE-A, constructed by Surrey Satellites Technology Limited (SSTL), was not launched until 2005 (European Commission, 2006b: 3). This satellite was ‘retired’ in July 2012 and moved to an altitude of 23,200km, where it is engaged in monitoring radiation in MEO (Satnews.com, 2012). The first two Galileo satellites were launched into orbit on 21st October 2011, as part of the In-Orbit Validation (IOV) phase (Amos, 2011), which continued with the launch of two more satellites in October 2012. The first successful positional fix using only Galileo satellites and ground stations took place on the 12th March 2013, marking a significant milestone in the development of programme (European Space Agency, 2013c). Not only was the event the first time a European system had provided a positional fix, establishing independence from other GNSS operators, but it also indicated that the system was functioning as expected. On the 22nd August 2014 the fifth and sixth Galileo satellites – the first classed as having Fully Operational Capability (FOC) – were launched from Kourou in French Guinea on-board a Soyuz launcher with intended orbits of 29,900km altitude and 55° inclination. However, it was revealed shortly after the launch – which was initially announced as successful – that the Galileo satellites had been placed into an anomalous elliptical orbit with an apogee of approximately 26,200km and an inclination of 49.8° (Arianespace.com, 2014; Clark, 2014). At the time of writing it remains unclear whether any correctional manoeuvres may be possible and what impact the incorrect orbit will have on the satellites' operations.

Galileo was preceded by EGNOS, a Satellite-Based Augmentation System (SBAS) which represented the first generation European GNSS, otherwise known as GNSS-1 (Eurocontrol, 2010b; Pasco, 2009).[31] The EU was not the only actor working on a SBAS: the US had a system called the Wide-Area Augmentation System (WAAS) and the Japanese the Multi-transport Satellite-based Augmentation System (MSAS) (European Commission, 2006a: ix). The development of these systems influenced the planning for the European GNSS-2 project; in its February 1999 Communication, the EC considered cooperating with Japan on Galileo as negotiations had already successfully taken place between the two actors to ensure interoperability between their respective augmentation systems (European Commission, 1999: 6).

EGNOS became operational in 2009 and augmented the existing GPS C/A Code by providing "correction and integrity information intended to improve positioning, navigation and timing services over Europe" (European Commission Directorate-General for Energy and Transport, 2009: 5). The system uses 40 ground stations across Europe and North Africa, and 3 geostationary satellites to increase the accuracy of existing GPS signals in those regions. Again, the need for competition with and independence from GPS appears as a justification for the development of EGNOS and Galileo, particularly given that there is "no guarantee of service" (European Commission, 2010: 2) from GPS.

One of the primary applications for EGNOS is in the aviation sector, for which it was approved in 2011. The EC planned and developed the system alongside ESA and the

---

[31] GNSS-1 is the general term for first generation systems which augment existing GNSS services in a specific geographical region, while Galileo is the European GNSS-2 (second generation) project: an independent GNSS with worldwide coverage.

European Organisation for the Safety of Air Navigation (Eurocontrol) (Eurocontrol, 2010a; European Space Agency, 2012g). This cooperation suggests that the project was, from the very beginning, conceived to offer significant opportunities for improving European aviation safety, and in particular, the usage of both EGNOS and Ground-Based Augmentation Systems (GBASs) to increase the accuracy of aviation navigation and enabling pilots to make more informed decisions for landing approaches through its Safety of Life (SoL) service (European Commission Directorate-General for Enterprise and Industry, 2011; European GNSS Supervisory Authority, 2009: 1).

Aviation is not, though, the only area to which EGNOS is being applied. The various areas in which GNSS services can be employed are also enhanced through the use of SBASs. Consequently, EGNOS is used throughout Europe to assist a large number of applications, including but not limited to: agriculture, scientific research and transport (European Commission, 2006b). Additionally, Europe is not the only region where EGNOS could be employed. In the 7th Space Council resolution, the Council of the European Union:

> [acknowledges] the potential value added of EGNOS for air transport safety, economic development in Africa and intercontinental exchanges; and [… invites] the European Commission to work with the African Union Commission capacity building in this area and the way a similar infrastructure to EGNOS could be implemented in Africa (Council of the European Union, 2010: 11).

The efforts detailed above to expand EGNOS capabilities to Africa fits with the EU's ambitions for leadership. While there is certainly a humanitarian aspect involved, the opportunity to expand EGNOS would place the EU in a prime position to claim global leadership of augmented navigation systems.

From the beginning of the operational phase, Galileo is expected to provide three signals: the Open Service, which is a free signal for widespread usage; the PRS, an encrypted signal for use by governments and organisations engaged in critical transport and emergency services, law enforcement and border control; and finally a SAR service, which will provide accurate data for the location of alert and distress signals. The Commercial Service will be tested after the operational phase begins, with the intention being for it to be provided once the full constellation is in orbit (European Commission Enterprise and Industry, 2013).

As mentioned earlier, the EC intended for Galileo to be interoperable with GPS. In this light, negotiations took place between the EU and the US during the early 2000s over interoperability between the two systems. In December 2001, US Deputy Secretary of Defence Paul Wolfowitz wrote to NATO members requesting that they put pressure on the EC to stop Galileo, or at the very least ensure that the planned GNSS could be jammed by the US in a manner that would not affect the GPS military signals (Bolton, 2012: 198). Bolton (2012) notes that after this request seemingly met little or no response, the US changed its strategy to ensure that the planned M-Code would not be compromised (p. 198). Specifically, there was concern on behalf of the US that the Galileo programme was intending to use a frequency which had been earmarked for the M-Code (Trimble, 2003). Although the EU eventually agreed to use a different frequency,[32] the disagreement highlights the competitive nature of outer space affairs, even when the ultimate objective is interoperability. At the time of writing, ensuring compatibility and interoperability between EGNOS, Galileo and other GNSSs remains prominent within the EU's plans; it would

---

[32] For a detailed account of the Galileo-GPS negotiations, see Bolton (2012).

appear that such compatibility and interoperability is to be agreed upon through bilateral international agreements with actors operating GNSSs (see European Parliament and Council of the European Union, 2013: L 347/10). Notably however, the European Parliament and Council of the European Union (2013) stress that compatibility and interoperability between EGNOS, Galileo and other GNSSs should take place "without prejudice to the objective of strategic autonomy" (p. L 347/3).

3.6 Copernicus

Unlike Galileo, Copernicus is not replacing an existing non-European capability or service. Nor is it based purely in outer space (European Commission, 2008). While Galileo has been developed as a response to concerns over increasing European dependence upon GPS, "the underlying principles of GMES[33] are", as Pasco (2009) argues, "to promote a convergence between the political (even social) demand for technology and the supply of that technology" (p. 15). In other words, Copernicus was born out of a perceived need to utilise Earth observation technologies based in outer space to assist terrestrial non-military security efforts (see Council of the European Union, 2000; European Commission, 2008; 2009).

For the EU, the potential security applications of outer space technologies – and particularly Copernicus – extend well beyond military objectives; as Robinson (2011a) notes, they include "space-based systems for environmental concerns, energy security, crisis management, peacekeeping, civil protection and other areas" (p. 3). In this way, Copernicus contributes to the securitisation of terrestrial life through outer space (Peoples, 2010; 2011). In other words, Copernicus reflects the securitisation of scientific Earth observation technologies as they are being channelled into supporting a multitude of non-

---

[33] The GMES programme was renamed 'Copernicus' in December 2012.

military security projects. In addition to environmental security efforts, these projects include, but are not limited to, “maritime surveillance, border control and support for EU external actions” (Council of the European Union, 2010: 8).

Copernicus will not rely on assets and services based solely in outer space. The project comprises of both outer space and *in situ* sensors, with the former relying on a combination of existing national extra-terrestrial scientific infrastructures and Copernicus-specific Sentinel satellites, while the *in situ* component uses “a large number of facilities, instruments and services owned and operated at national, regional and intergovernmental levels inside and outside the EU” (European Commission, 2008: 3). Last but not least, the services component will involve the dissemination of data collected from the outer space and *in situ* components. Importantly, Copernicus is not solely an EC-ESA project like Galileo, as other EU institutions and member states have a vested interest in the programme: the European Organisation for the Exploitation of Meteorological Satellites (EUMETSAT), for example, owns and operates the satellites planned to be used for the meteorology dimension (European Commission, 2008; 2009).

The space component of the Copernicus programme will, once launched, comprise of up to 10 ‘Sentinel’ missions. Four of the missions will have two satellites, ‘A’ and ‘B’, whilst Sentinel-5 will have a precursor mission in addition to its ‘A’ satellite (European Space Agency, 2012b) housed within the TROPOspheric Monitoring Instrument (TROPOMI) satellite (European Space Agency, 2014e) (see figure 3.2 for general details of each mission). Unlike the first three Sentinel missions, Sentinels-4 and -5 will be housed on meteorological satellites operated by EUMETSAT (European Space Agency, 2014e). The purpose of the Sentinel-5 precursor mission is to avoid a gap in atmospheric monitoring data between Envisat and the Sentinel-5. However, following the sudden malfunction of Envisat on the 8th April 2012 (see Amos, 2012b) and subsequent unsuccessful attempts to resume communications with the satellite, ESA declared on the 9th May 2012 that the mission had ended (European Space Agency, 2012a). The Sentinel satellites are being developed by a consortium of European space industry companies: Thales Alenia Space Italy is the prime contractor for Sentinel-1, with contributions from Astrium Germany and Astrium UK; Astrium is the prime contractor for Sentinel-2; whilst Thales Alenia Space is again prime contractor for Sentinel-3 with contributions from Astrium for the payload (Astrium, 2011; European Space Agency, 2014b; 2012d; 2012e; 2012f).

Mission	**Orbit**	**Instruments**	**Purpose**	**Planned launch for first satellite**
Sentinel-1	Polar-orbit	Synthetic Aperture Radar	Land and ocean monitoring	Launched (3rd April 2013)
Sentinel-2	Polar-orbit	Multi-spectral high-resolution imaging	Land monitoring and emergency services	2014
Sentinel-3	Polar-orbit	Multi-instrument	Atmospheric, land, ocean and topography monitoring	2014
Sentinel-4	Geostationary	Multi-instrument	Atmospheric monitoring	2019
Sentinel-5 precursor	Polar Orbit	Multi-instrument	Atmospheric monitoring	2016
Sentinel-5	Polar Orbit	Multi-instrument	Atmospheric monitoring	2020

Figure 3.2 The Copernicus space segment. Data from European Space Agency (2013e; 2013f; 2014b; 2014c; 2014d; 2014e; 2012a)

One of the objectives of the Copernicus project is to unify and strengthen existing European Earth observation programmes. The objectives are still in progress of being completed, according to an EC Communication in 2005:

> Europe has developed world class assets and expertise. However, observing systems are run independently and coverage is incomplete for both the in-situ and satellite observing systems. Many satellites and in-situ observing networks are experimental and cannot guarantee the required quality and continuity of measurement to provide the basis of operational services now or in the future (European Commission, 2005: 3).

By initiating a collaborative effort between EU Member States, the EC, ESA and other EU organisations, the EU was clearly stating its intentions to strengthen the European space industry and European scientific autonomy whilst simultaneously promoting its bid for leadership in using Earth observation technologies for civil security applications (see European Commission, 2005). Copernicus is not the only example of such an endeavour in the field of Earth observation. The Multinational Space-based Imagery System (MUSIS), although a military project, is a collaboration between seven European states – Belgium, Germany, Greece, Spain, France, Poland and Italy (European Defence Agency, 2011) – intending to pool their Earth observation resources and avoid the duplication of technologies and capabilities. However, progress has been hampered by difficulties agreeing which states should undertake which Earth observation functions. (Norris, 2010: 207). In this sense, Copernicus is arguably advantaged by the decision to use a separate set of missions – the Sentinels – for its space component. This approach does not require EU Member States to cancel or alter their own Earth observation capabilities by necessitating the avoidance of duplication, a state of affairs furthered by the fact that no Sentinel satellites will have a resolution smaller than 10m (Anonymous, 2012a), thus not competing with existing EU Member State missions.

A minor digression is necessary to briefly explain the two general forms of Earth observation imaging technologies. Earth observation is arguably an aspect of remote sensing, which itself has many varying definitions,[34] although for the purpose of this thesis, a relatively general definition will suffice. Lintz and Simonett (1976a) choose to describe remote sensing as "the acquisition of physical data of an object without touch or contact" (p. 1). However this definition is, as Harris (1987) notes, "too broad, and […] could be construed to include reading a thermometer" (p. 2). A slightly more specific and appropriate definition is that proposed by Lillesand and Kiefer (1987): "[r]emote sensing is the science and art of obtaining information about an object, area, or phenomenon through the analysis of data acquired by a device that is not in contact with the object, area, or phenomenon under investigation" (p. 1). Other, more specific definitions have been proposed, however the limitations they impose on the technologies used in remote sensing or the objects studied restrict their suitability in the context of Copernicus. In this light, it could be argued that Earth observation pertains to the remote sensing of the Earth, with studies of extra-terrestrial objects falling under other categories. Although the term Earth observation implies that some form of physical surveillance is being undertaken, missions of this kind are not limited to imaging satellites, though these are the most common.

There are two variants of imaging satellites: optical and radar. The capabilities of these variants are outlined in figure 3.3, but the most effective Earth observation data is derived from a combination of optical and radar satellite missions (Norris, 2010: 218). For instance, while radar satellites can provide high resolution images, those images are subtly different to data from optical satellites. Because of the characteristics of radar, the images display the reflection of radio signals emitted by the satellites, rather than reflection of

---

[34] See Campbell and Wynne (2011: 6) for a list of increasingly complex and specific definitions of remote sensing.

light, as in optical imagery. Consequently, whilst radar imaging satellites can see through clouds and darkness, the pictures they return can sometimes obscure the reality of a situation; Norris (2010) notes that a smooth surface, such as calm water or dry sand, usually appears black on a radar image due to the absence of radio signals reflected back to the satellite, no matter which colour they actually are. Although the resolution of the images provided by Earth observation satellites is significant, what is arguably even more important is the revisit time of a satellite. The revisit time is, as its name suggests, the time it takes for a satellite to pass over an area more than once. Ideally, the revisit time should be as low as possible, so that movement or changes in a particular area can be detected quickly and reliably.

Capabilities	**Optical**	**Radar**
High Resolution (< 5m)	x	x
Multi-spectral imaging	x	
All-weather imaging		x
Detailed night-time imagery		x

Figure 3.3 Remote sensing imaging variants

Sentinels aside, most existing European Earth observation missions are either designed for military or dual-use purposes. The French Helios-2 satellites are high-resolution optical military satellites capable of 35cm resolutions (Norris, 2010). France is also a partner with Italy in the Optical and Radar Federated Earth Observation (ORFEO) programme, which uses the French Pléiades missions for optical surveillance and the Italian Cosmo-Skymed for radar observation data. There are also data-sharing agreements between France and Sweden, Belgium, Spain and Austria for data produced by the Pléiades satellites (Centre National D’Études Spatiales, 2012). Another advantage of

Pléiades is its manoeuvrability: when Envisat – the European polar-orbiting Earth observation satellite which replaced the European Remote Sensing (ERS) satellites – suddenly malfunctioned in April 2012, Pléiades was tasked to capture an image of the stricken satellite (Amos, 2012b). The German SAR-Lupe system is a set of five radar satellites providing 50cm resolution on captured images for military purposes. The constellation of five satellites also means that there is a fairly short revisit time: 36 hours at most (Norris, 2010: 216).

Envisat itself was launched by ESA in March 2002 with the objective of providing "measurements of the atmosphere, ocean, land and ice" (European Space Agency, 2012c). Until it officially ended in May 2012, it was one of a number of ESA Earth observation missions, with others including CryoSat, ERS (the precursor to Envisat), the Gravity field and Ocean Circulation Explorer (GOCE), Proba and the Soil Moisture Ocean Salinity (SMOS) mission, although GOCE and SMOS do not use any imaging technologies. The aforementioned missions are managed and operated by ESA, separating them from the national missions mentioned above. Copernicus will support existing Earth observation missions, including the ESA missions listed, either by offering additional data to what is currently available, or, in the case of Sentinel-5, by replacing existing missions when they end their operational lifetimes.

Returning to Copernicus, the path to the completion of the project has been by no means straightforward. In June 2011, the EC announced that the Copernicus project would not be included in the proposed Multi-annual Financial Framework (MFF) for the period 2014-2020 as "the costs and/or cost overruns are too large to be borne only by the EU budget" (European Commission, 2011b: 21). Under this plan, the financing of the project would depend upon direct contributions from EU Member States, which in a time of recession may well struggle to persuade their populations of the importance of contributing to Copernicus. This proposal, unsurprisingly, raised significant objections from ESA and EU Member States, including a letter sent to the EC in November 2011 signed by ministers from France, Germany, Italy, the Netherlands, Spain, Sweden and the UK (de Selding, 2011a; 2011b). By June 2012, no firm decision had been made over Copernicus funding, with the EC deferring one until later in 2012 or 2013 (de Selding, 2012c). This put pressure on ESA, which stated in February 2012 that it needed confirmation over the Copernicus budget by June of that year in order to decide itself whether to commit to the launch of Sentinel-1A, scheduled for 2013 (de Selding, 2012b). ESA had considered putting Sentinel-1A into storage until funding had been confirmed (Amos, 2012a; de Selding, 2012b) though in end this did not take place. The impasse over funding was particularly inconvenient given the failure of the Envisat mission in May 2012 mentioned earlier. Although the Sentinel-1 mission carries different instruments to Envisat and is charged with different objectives, any continued doubt over Copernicus financing had the potential to delay progress on subsequent missions, including Sentinel-3, Sentinel-5 precursor and Sentinel-5, which are intended to enhance or replace the data-stream from Envisat.

In June 2012 there was yet another twist in the tale: ESA came under pressure from clients and Earth observation data users to replace, with the utmost expediency, the data streams which had been lost with Envisat (de Selding, 2012a). This led to the decision by ESA to reserve a launcher with Arianespace, with a view to launching Sentinel-1A in 2013 as originally planned. The situation was resolved in February 2013 when Copernicus was eventually included within the MFF for the period 2014-2020: €3.786 billion of EU funding was dedicated to the programme (European Council, 2013: 9), ensuring that there would be no further imminent concerns over finances. It should be noted however that this figure falls short of the €5.481 billion estimated to be the “maximum financial envelope” required for the programme in a 2012 Communication from the EC (European

Commission, 2012c: 3). On the 3rd April 2014, the Sentinel-1A satellite was launched from the Arianespace facility in Kourou, French Guiana (European Space Agency, 2014b), with the introduction of the space segment to complement *in situ* data sources marking an important stage of the Copernicus programme.

3.7 Galileo and Copernicus: Future European critical infrastructures

As has been charted above, both the Galileo and Copernicus projects have had complicated beginnings. Nonetheless, it would appear that the Galileo project, after over a decade of negotiations and political comprise, is on its way to becoming a reality, while the future of Copernicus seems assured now that long-term funding has been guaranteed. Although the various satellite assets may not yet be in place, the services for both programmes have been decided upon, meaning that it is possible to categorise both Galileo and Copernicus as future European critical infrastructures.

3.7.1 Galileo as a critical infrastructure

Once complete and operational, Galileo is expected provide a host of reasonably accurate signals for civilian use, as well as dedicated SAR and specialised services tailored for use by governments. It should also bring in a substantial amount of revenue for the EU and assist the growth of businesses and industry throughout Europe. However, Galileo also represents, as mentioned earlier, an independent European capability in the area of GNSS services. Although this in itself does not make Galileo a critical infrastructure for the users of the services, that independence is necessary for the long-term ambitions of the EU to "**exert global leadership in selected policy areas in accordance with European interests and values**" (European Commission, 2007b: 4, original emphasis). Although GPS provides a similar service to Galileo, particularly when the planned upgrades to the

US system are completed in the next few decades, the chance that GPS signals could be withdrawn at the whim of the US restricts the EU's ambitions for global leadership. Galileo can therefore be considered critical at the political level, even if the benefits it provides to the EU in that respect do not make it a critical infrastructure in terms of its relationship with the smooth-running of societies and states on Earth.

Since this thesis is investigating European outer space security practices, the definition employed here with regards to critical infrastructures will be that of the Council of the European Union (2008a: L 345/77). As discussed earlier in this chapter, determining the criticality of an infrastructure is not simply a case of assessing whether that infrastructure provides a unique and important service or services, but also the extent to which its services are acknowledged as supplementing and supporting other infrastructures. In the case of Galileo, as with Copernicus, the programme is in the process of being developed and deployed and therefore it cannot be known with any certainty what wider socio-political and –economic effects or applications its services will have. Nonetheless, some assumptions can be made based on the predictions of the EC and the existing example of GPS. Before proceeding with the analysis of the criticality of Galileo, it is worth briefly noting the unpredictability of future technological innovations and developments. GPS, as mentioned earlier, is a military programme operated by the US government, although it is now an integral part of both commercial and non-commercial civilian life. On the orders of President Reagan following the downing of flight KAL-007 by the USSR in 1983, the GPS C/A code was made available to civilian aircraft worldwide upon completion of the GPS constellation (Pace *et al.*, 1995: 263; Speakes, 2009).[35] This

---

[35] Although it is widely reported (see, for example, Rip and Hasik, 2002: 429) that the decision to make GPS signals available to civilian aircraft was issued through a directive, it appears that the only public announcement by the Reagan administration at the time was a statement to the press on September 16th 1983, which established that "the United States is prepared to make available to civilian aircraft the facilities of its Global Positioning System when it becomes operational in 1988" (Speakes, 2009).

decision, although made ostensibly to avoid the repetition of an event like that of KAL-007, led to the rapid expansion of commercial applications associated with GPS signals, which in turn was a significant factor behind the decision of the EU to pursue the development of an independent GNSS. The point to be emphasised is that future technological and socio-political developments may lead to GNSS signals being used for currently unforeseen purposes or applications.

To begin with the civilian signals that an operational European GNSS will provide, the EC lists a series areas with which it expects EGNOS and Galileo services to assist and improve, including:

> Handsets and mobile phones […] Civil protection and surveillance […] Energy […] Mapping and land management […] Synchronisation of networks […] Meteorology and disaster prevention […] Precision agriculture and environment […] Fishing […] Logistics […] Rail […] Urban transport […] Road transport […] Maritime transport [… and] Aviation (European Commission, 2010: 6)

This list represents a long-term expectation of GNSS applications and consequently not all of these areas will be affected to the same extent by EGNOS and Galileo, however it is indicative nonetheless of the wide-ranging influence that GNSS services have. It should be noted though that, with the possible exception of the ‘synchronisation of networks’, none of these areas necessarily depend upon the provision of GNSS signals; rather, they enjoy the benefits of accurate timing and positioning signals but can operate without them. There is not the space within this chapter to go into great detail on how Galileo, and in some cases EGNOS, may affect all the areas included on the EC’s list. Therefore, what follows is an examination of what benefits may be provided to the areas which the EC expects EGNOS and Galileo to be the most valuable: aviation, fishing, maritime and road transportation and the synchronisation of networks (European Commission, 2010: 6).

As mentioned earlier, EGNOS is already in use with regards to aviation in Europe, offering more accurate positioning signals to aircraft through its Safety of Life service in order to improve effectiveness, efficiency and safety. Aircraft do not require GNSS signals to navigate or fly – as explained above, GPS signals were only made available to civilian aircraft in the 1990s – but the increased accuracy of three dimensional positioning means that air transportation is now much more efficient than it was previously, both in the air and on the ground. In particular, approach procedures and navigation around airports have been improved through more accurate GNSS signals, particular those provided by EGNOS (European Commission Directorate-General for Enterprise and Industry, 2011). The increase in airspace capacity in turn enables more aircraft to fly, transporting more people and, perhaps more relevant to the nature of this discussion, more goods. To take a fairly broad view, increased efficiency within the aviation sector benefits commerce and tourism and thus state economies and the finances of state populaces. The Galileo programme is also expected to be integral to future European Air Traffic Management (ATM) and is considered integral to a number of aspects of the on-going Single European Sky ATM Research (SESAR) project (European Commission, 2007a). Bearing in mind that the criticality of infrastructures is often determined by the "necessarily *negative*" (Burgess, 2007: 475, original emphasis) approach of evaluating the impact their disruption or destruction would cause, the loss of GNSS signals may not cripple the aviation industry outright. However, it may well have a severe impact upon the number of flights that could be managed in the air and at airports, as well the safety of aircraft and their abilities to navigate terrain and weather formations. Equally, while an abrupt restriction of the aviation sector may not prove disastrous to the survival of states, it is safe to assume that there would be a significant disruption to the conduct of financial and commercial affairs. It would appear then that while GNSS signals are not integral to aviation, insofar as their disappearance or disruption would not necessitate a grounding of all aircraft throughout affected regions, they are critical to the maintenance of current levels of traffic and it is conceivable that their loss may have a ‘significant impact’ upon states.

Maritime navigation and fishing will for the purposes of this chapter be considered in tandem, as the benefits to these sectors are broadly similar. The main applications of Galileo to these sectors revolve around improved positioning signals, both on the high seas and near and within harbours, with the objective being to enable more effective and efficient sea-borne transportation, particularly in poor meteorological conditions. As with aviation, maritime navigation is, of course, possible without the provision of GNSS signals – evidence of this dates back millennia – but it cannot be denied that accurate positioning data improves safety and efficiency. Whether or not this will make Galileo a critical infrastructure when it comes into service is another matter however. Unlike aviation, an accurate three-dimensional positioning signal is not in itself critical to maritime transportation, although it should be noted that the EGNOS SoL service is considered applicable to the maritime sector (Kaplan and Hegarty, 2006: 562), indicating that augmented and reliable GPS signals are considered important if available. Maritime navigation is often augmented using a number of systems, including EGNOS, WAAS and the Maritime Differential Global Positioning System (MDGPS) (Kaplan and Hegarty, 2006: 14), which are all available within specific geographical regions. These augmentation services, which include both GBASs and SBASs, enable vessels to navigate near the shoreline and through major waterways efficiently and safely, as the crew has an accurate understanding of their position in relation to geographical locations and other vessels. The benefit of these augmented signals for the fishing industry is a more accurate awareness of a ship's position, meaning that crews can use their time more efficiently and effectively, which may well lead to an increase in hauls and, consequently, income. In addition, the use of GNSS receivers on fishing trawlers allows improved regulation of the industry, ensuring that the sustainability of fishing can be monitored (European Commission, 2006b: 7). It is debatable though whether or not this qualifies such services as 'critical'; the improved efficiency and sustainability of marine transportation and fishing enabled by GNSS signals are certainly beneficial to European societies, however the extent to which the loss or disruption of those signals would have a 'significant impact' upon a Member State remains questionable. Certainly, from an economic and industrial perspective, marine transportation and fishing are valuable sources of commerce and income, meaning that they could be considered critical infrastructures insofar as they maintain the economic welfare of certain societies. The question then is whether the loss or disruption of GNSS services would have an impact on marine transportation and fishing significant enough to threaten, or be acknowledged to threaten, the livelihoods and economic stability of societies dependent upon those forms of income. If a Member State were to deem the GNSS services supporting and improving marine transportation and fishing as critical to the economy and welfare of their population, then those services and the GNSS providing them become, in value even if not in name, critical infrastructures.

Another important means through which GNSS services, and particularly Galileo, can assist marine transportation is improved SAR capabilities. Galileo will act as the EU's contribution to the existing international space-based SAR service, known as Cospas-

Sarsat,[36] which involves a number of satellites located at different orbital altitudes working to relay signals from the personal beacons of anyone stranded at sea. The main planned improvement to existing SAR services is the transmission of information back to the beacons of those stranded. The current process is purely unidirectional; positioning information is relayed through the network of satellites to the ground stations and then on to SAR teams. It is intended that Galileo, as well as reducing the time for information relayed to the ground stations, will be capable of transmitting information or feedback to the user of the beacon (European Space Agency, 2014b). In terms of the criticality of Galileo, this service is expected to be unique, at least in the short-term, meaning that its loss or disruption would have a significant impact upon the conduct of SAR operations. Nonetheless, the fact that such operations are being conducted successfully at the moment indicates that although certainly an added benefit to SAR, the shortened relay time and transmission of feedback to beacon users is not a necessity.

The European road transportation sector is also expected to benefit greatly from Galileo. The main advantage of GNSS signals providing improved accuracy to road-users is, similar to aviation and marine transportation, an increase in efficiency. However, Galileo's services will also contribute to the wider European Spatial Development Perspective (ESDP) and, in particular, the Trans-European Transport Network (TEN-T). These two policies involve a specific spatial imagination of Europe towards which the EU is directing its policies. An important part of the vision present within the ESDP is a spatio-temporal reduction in the size of Europe through improved road and rail transportation, enabling faster and more efficient travel across the region. In other words, Europe will be 'squeezed' as infrastructural improvements reduce the time it takes to

---

[36] Cospas stands for 'Cosmicheskaya Sistyema Poiska Avariynich Sudov', which translates from Russian as 'Space System for the Search of Vessels in Distress' and Sarsat stands for 'Search and Rescue Satellite-Aided Tracking' (National Aeronautics and Space Administration Goddard Flight Center, 2000: 2)

journey between places (Jensen and Richardson, 2004). Although much of the TEN-T requires a centralised organisation and co-ordination of European road and rail networks, the enhanced accuracy of Galileo's positioning and navigation signals over the existing GPS constellation has the potential to improve the flow of traffic. This can largely be achieved by mitigating congestion and increasing road safety by navigating drivers along the shortest or quickest routes to their destinations (European Commission Mobility and Transport, 2012). With respect to the criticality of the Galileo project to road transport, the situation is similar to that of aviation and marine transportation; providing the planned applications are successful, the increased accuracy of the positioning signals transmitted by the Galileo constellation will certainly improve movement on Europe's road networks but the disruption of those signals will most likely not prove catastrophic. If anything, the safety benefits which should be provided by Galileo are not as relevant to road transportation compared with movement in the air and on the high seas, given the necessity for an accurate knowledge of positioning present in the latter two forms of transport.

The final area to which Galileo is expected to contribute greatly is the synchronisation of networks. GNSS constellations require a high level of timing accuracy in order to offer reliable positioning data and are therefore capable of providing synchronisation signals to users. These signals are crucial to a number of terrestrial services, from energy infrastructures to communications and financial networks (European Commission, 2013b: 13). If anything, this service is one of the most important contributions that Galileo will provide to terrestrial critical infrastructures and LTSs. The synchronisation of timing enables a network spread across a large geographical area to function smoothly; for instance, telecommunication networks depend upon synchronisation for servers and security measures such as encryption (Galileo Joint Undertaking, 2005: 4). While timing and synchronisation signals are already offered by other GNSS operators, Galileo’s signals, in addition to an expected increase in accuracy (Galileo Joint Undertaking, 2005: 4), will offer another source for network synchronisation, increasing redundancy in the event of a disruption in one of the GNSSs. In terms of criticality, the existing synchronisation capability of the GPS constellation demonstrates that the provision of these services by Galileo will not be unique or irreplaceable in case of failure. Nonetheless, even if the increase in accuracy over competitors is not as large as expected, particularly once the GPS III upgrade is completed, the redundancy introduced by Galileo is a significant factor, making it an important component in the operations of terrestrial critical infrastructures.

In a 2013 Commission Staff Working Document, the EC notes that “[a]ny shutdown of even a part of space infrastructures could have significant consequences for the well-functioning of economic activities and our citizens’ safety and security, and would impair the provision of emergency services. This is particularly true for Galileo” (European Commission, 2013b: 13). However, although many of the services offered by Galileo may offer improvements over existing GNSS signals, the majority are not necessarily unique. Nonetheless, the expected interoperability with GPS means that eventually there will be a significant increase in the redundancy available for the services offered by both Galileo and its US competitor. The bi-directional SAR services that Galileo will provide are an exception though, as this capability does not currently exist and thus it is reasonable to assume that a disruption may well “impair the provision of emergency services” (European Commission, 2013b: 13). In this sector then, the European GNSS will most likely be a vital component in the conduct of future SAR operations. However, this does not necessarily make it a critical infrastructure; although SAR is undoubtedly an important component of maritime activities, it is unlikely that the “disruption or destruction” of Galileo’s bi-directional services would “have a significant impact in a Member State" (Council of the European Union, 2008a: L 345/77). This being said, it can be argued that the European independence offered by the Galileo programme transforms it from a purely interoperable system to a critical one. A 2010 EC Communication reiterates the importance of an independent system, contending that "[a]pplications based on EGNOS and subsequently on GALILEO would make a decisive contribution to the development of a knowledge-based society and the creation of high-value jobs in the EU" (European Commission, 2010: 3). In other words, in addition to the 'direct' navigation and positioning services of Galileo, the economic benefits of a European GNSS will be significant. Indeed, throughout the development of the programme, commercial and economic growth was one of the main justifications proposed by the EU for the substantial investment required.

As mentioned earlier in this chapter, the 2013 Commission Staff Working Document emphasises the importance of interdependencies between "critical infrastructures, industry, and state actors" (European Commission, 2013b: 1). Although the document quotes the definition of ECIs provided by the Council of the European Union (2008a: L 345/77), this "new approach" (European Commission, 2013b: 1) exploring intra- and inter-sector interdependencies arguably breaks away from the existing definition of ECIs. As discussed above, the Galileo programme does not comply with the Council of the European Union's definition of ECIs as it only offers one unique service: the bi-directional SAR signals. The remaining services, although crucial to a number of other critical infrastructures, are replications of existing GNSS services, albeit ones offering independence from non-European GNSSs such as GPS. Given the planned Galileo-GPS interoperability, a hypothetical disruption of Galileo's services would only become an issue for users in the occasion that GPS were to be simultaneously disrupted. If navigation, positioning and timing signals from one of the GNSSs were to stop, the other system would act as a redundancy. Consequently, there are two possible implications from the explicit designation of Galileo as a critical infrastructure: either that GNSSs are critical infrastructures, regardless of redundancies existing through other systems; or that the existence of non-European systems are excluded from assessments of criticality regarding the provision of navigation, positioning and timing signals for European societies. Of these possibilities, the second is arguably the most likely, given the emphasis on independence present within EU documents related to the Galileo programme. In other words, the continued access to GNSS services provided by a European system is being prioritised ahead of the redundancies provided by expected Galileo-GPS interoperability.

The access to independent navigation, positioning and timing signals which Galileo provides is also critical to the EU's wider ambitions for space power projection. Peter (2010: 353) includes the need for a European GNSS in his list of areas Europe – by which he means the EU, ESA and their respective Member States – needs to improve in order to expand its space power. Not only will Galileo provide support for the regional and domestic policies of the EU and its Member States respectively, but it will arguably be symbolic of European industrial and scientific might. This is particularly important given that at the time of writing it remains the only civilian-operated GNSS with the express objective of global coverage. By displaying such industrial and scientific capabilities through a successful Galileo programme, the EU would be working to establish the legitimacy of its leadership in outer space affairs.[37] The argument can thus be made that from the perspective of the EU as an institution, any long-term disruption to Galileo's infrastructure may have a damaging effect upon its leadership ambitions.

---

[37] See the discussions on consensual recognition of legitimacy and non-military power projections in chapter 2 of this thesis.

As mentioned earlier, future technological innovations may well lead to new applications emerging for Galileo. At the time of writing however, the most significant advantage it provides the EU is expected access to a substantial commercial market worth around €124 billion in 2008 and estimated to provide revenues of between €55-63 billion for EU Member States over the next 20 years (European Commission, 2010: 2-3). Consequently, solely from the perspective of the economic benefits of Galileo, it can be argued that the programme will become a critical infrastructure once operational, as a disruption in its services would likely have a significant impact on European commerce.

The EU appears to be determined to establish Galileo's credentials as a critical infrastructure (see European Commission, 2013b: 13), despite – with the exception of bi-direction SAR services – the fact that programme will not provide necessarily unique GNSS services that taken individually would lead to a "significant impact in a Member State" (Council of the European Union, 2008a: L 345/77) in the event of their disruption. Nonetheless, considering the improved accuracy of navigation, positioning and timing signals that Galileo is expected to provide, the opportunity for independence from non-European GNSSs it offers, the financial and policy-multiplication opportunities for the EU, and the redundancy for users worldwide offered by interoperability with the US, the argument can be made that, taken as a whole, the programme will offer enough benefits that a disruption to its services once operational may well have significant impacts on EU member states. Moreover, as this thesis is questioning whether the EU considers Galileo to be a critical outer space infrastructure, it would appear that this is indeed the case, as evidenced by the inclusion of the GNSS in a pilot programme addressing intra- and inter-sectoral interdependencies amongst critical infrastructures (see European Commission, 2013b). Although Galileo cannot be considered an ECI as it does not comply with the existing definition of that term for a number of reasons discussed above, the argument can be made that once operational, it will be a European critical outer space infrastructure.

3.7.2 Copernicus: complementary yet critical services

Unlike Galileo, Copernicus does not, at first glance, offer services which could be deemed critical to the extent that their loss would result in severe disruption for states and organisations receiving them. As mentioned earlier, when fully operational the Copernicus programme is expected to employ a combination of orbital and *in situ* sensors. These sensors provide data pertaining to a range of applications largely focused around the six general themes of the programme: land monitoring, marine monitoring, atmospheric monitoring, emergency management, security and, last but not least, climate change (Copernicus.eu, 2013d). Many of the projects associated with the Copernicus programme involve a focus upon sustainability, in line with the Seventh Framework Programme for Research (FP7), which has an "overarching aim […] to contribute to sustainable development" (The European Parliament and the Council of the European Union, 2006: L 412/7). According to Annex I of The European Parliament and the Council of the European Union (2006) decision concerning FP7, Copernicus, or GMES as it was then called, was originally expected to involve the:

> development of satellite-based and in-situ monitoring and early-warning systems, including for the safety of citizens, and techniques relating to the management of the environment and security (including the management of natural disasters) and their integration with ground-based, ship-borne and airborne components; support for the integration, harmonisation, use and

> delivery of GMES data (both satellite-based and in-situ, including ground-based, shipborne [*sic*] and airborne) and services (p. L 412/25).

While the space-based and *in situ* components of the programme remain, the early-warning capabilities of Copernicus have been given little mention in recent documentation. Nonetheless, as discussed below with regards to the themes and projects of the programme, many of the services which are expected to be offered when Copernicus becomes fully operational will provide datasets which could be used for the early warning of environmental change on land, in the sea and in the atmosphere.

This section will briefly summarise the objectives of each theme and analyse criticality of the themes to users in Europe and around the world. As this thesis is exploring European outer space security, this section focuses upon the space segment of the Copernicus programme; although the criticality of each theme will be considered, particular attention will be given to the role of the Sentinel satellites and the potential disruption that may result from the loss of their services.

The land monitoring services for Copernicus are already operational, using existing space-based and *in situ* sensors to "provide land cover information to users in the field of environmental and other terrestrial applications" (European Environment Agency, 2012). According to the European Parliament and Council of the European Union (2010):

> Land monitoring services are important for monitoring biodiversity and ecosystems and support climate change mitigation and adaptation measures and the management of a wide range of resources and policies, most of which relate to the natural environment: soil, water, agriculture, forests, energy and

> utilities, built-up areas, recreational facilities, infrastructure and transport (p. L 276/3).

Whilst these services are undoubtedly important to long-term environmental sustainability and infrastructure management, they are not necessarily critical to European societies or EU Member States. In the short-term at least, the health and safety of European populations do not depend upon land monitoring to the extent that the disruption of those services would endanger societies. This is not to say that land monitoring capabilities are unimportant but they are by no means as critical as the navigation and positioning signals offered to aviation by Galileo, for example. Moreover, the fact that these services are already considered operational when the dedicated Sentinel satellites have not, at the time of writing, been launched could be considered evidence enough that the space segment of the Copernicus programme is not a critical infrastructure with regards to land monitoring. Although the Sentinel missions 1 through 3 will complement and improve upon existing land monitoring capabilities, it could be argued that the work being undertaken by the GMES In-Situ Coordination (GISC) project to coordinate and disseminate data from existing *in situ* sensors demonstrates that a disruption of the programme's space segment may not be catastrophic.

A similar argument could be made with regards to the atmospheric and marine monitoring capabilities that Copernicus will provide when fully operational. Although it is highly likely that some short-term applications will emerge from the datasets produced by the space-based and *in situ* components of the Copernicus programme, the objectives of these thematic areas are largely directed towards the long-term sustainability of the terrestrial and atmospheric environments. The atmospheric and marine monitoring services are described as producing "information for monitoring and understanding climate change and may contribute towards improvements in the transport sector and the deeper marine knowledge needed for implementation of the EU's new Integrated Maritime Policy" (European Commission, 2008: 4). It could be argued then that rather than providing services integral to the health and safety of European populations, the atmospheric and marine monitoring applications of Copernicus are intended to complement policy-making and existing initiatives promoting sustainability in the activities of EU Member States. Given their complementary nature, the atmospheric and marine monitoring services which will be provided by Copernicus cannot be considered critical to EU Member States despite their potential for policy-multiplication. However, the gap in atmospheric monitoring which emerged following the failure of Envisat in May 2012 demonstrates that the Sentinel missions dedicated to atmospheric and marine services will be vital to the applications and projects which they serve.

The emergency management services of the Copernicus programme have, as with those dedicated to land monitoring, been deemed operational since 2012 (European Commission, 2012c: 3). The objective of the emergency management component of Copernicus is to:

> provide information for emergency response in relation to different types of disasters, including meteorological hazards, geophysical hazards, deliberate and accidental man-made disasters and other humanitarian disasters, as well as the prevention, preparedness, response and recovery activities (The European Parliament and the Council of the European Union, 2014b: L 122/53).

It appears then that there are two sides to the emergency management services; on the one hand, the space-based and *in situ* sensors are assisting emergency responders following natural and man-made disasters – the humanitarian security aspect – while data from those sensors is also being used in long-term studies concerning “prevention, preparedness, response and recovery activities” (The European Parliament and the Council of the European Union, 2014b: L 122/53) pertaining to such disasters. With regards to the humanitarian security application of Copernicus, a number of FP7-funded projects are underway at the time of writing, one example of which is Increasing Resilience through Earth Observation (IncREO). The website of the Copernicus programme describes this project as attempting to:

> provide actors responsible for disaster management, risk prevention, civil protection and also spatial planning with EO-based solutions contributing particularly to an improved preparedness and mitigation planning for areas highly vulnerable to natural disasters and already noticeable climate change trends (Copernicus.eu, 2013a).

The focus of IncREO then appears to be on complementing and enhancing existing terrestrial emergency management measures through the improved coordination and dissemination of information gathered through remote sensing. Other on-going projects include the use of data from Copernicus with regards to volcanic activity and research into the short-term prediction of earthquakes (Copernicus.eu, 2013b). Turning then to the criticality of emergency management services offered by Copernicus, it could be argued that in some cases, such as projects dealing with predictions of earthquakes and volcanic activity, a hypothetical disruption might have more of an impact than a similar disruption of atmospheric, land and marine monitoring services. It should be emphasised though despite the increased criticality of these emergency management applications, they are still only designed to complement and enhance existing terrestrial capabilities for disaster and risk management. Furthermore, as with the land monitoring theme, the fact that these services are considered operational, and that a number of projects already under way prior to the launch of the Sentinel satellites, means that the dedicated space infrastructure of the Copernicus programme is not necessarily critical to the emergency management theme.

The final theme for which Copernicus is expected to provide services is, quite ambiguously, named ‘security’. Although there has been much political debate within the EU and ESA over the use of dedicated and dual-use outer space assets for passive military purposes (Pasco, 2009: 6), the security theme of the Copernicus programme involves border and maritime surveillance and the provision of support for the EU External Action Service “through the detection and monitoring of threats” (Copernicus.eu, 2013c; see also The European Parliament and the Council of the European Union, 2014b: L 122/53). In this fashion, Copernicus is contributing to the wider shift towards the anticipatory logic underpinning EU security practices mentioned earlier in this chapter (see De Goede, 2008b; 2011). One of the Copernicus projects of note associated with security is the GMES services for Management of Operations, Situation Awareness and Intelligence for regional Crises (G-MOSAIC), which lasted from 2009-2011 and addressed the border surveillance and EU External Action support objectives of the security theme. G-MOSAIC was financed largely by the EC through the FP7 and provided data for use in “early warning and crisis prevention” and “crisis management and rapid intervention” (gmes-mosaic.eu, 2010). Although G-MOSAIC was a pilot for future Copernicus security projects, the choice of services it provided arguably indicates some of the EU’s concerns regarding internal and external security threats. These services include the monitoring of critical infrastructures inside and outside the geopolitical borders of the EU, migration, nuclear facilities, treaty verification, the exploitation of natural resources, and, last but not least, crisis management and response. With regards to the criticality of these services, they are again largely complementary to existing efforts, offering improved coordination and dissemination of information. Moreover, it can be inferred from the absence of a dedicated Sentinel mission for the security theme that existing space-based and *in situ* sensors will be used for the future provision of operational services.

Although not a 'theme' of the Copernicus programme, it is worth noting that in addition to providing "spaceborne observations, serving primarily the [programme's] services" (The European Parliament and the Council of the European Union, 2014b: L 122/53), the space segment of the programme is also expected to provide "protection of satellites against the risk of collision taking into account the [European] Union space surveillance and tracking support framework" (The European Parliament and the Council of the European Union, 2014b: L 122/53). At the time of writing it is not clear how the Copernicus programme's space segment will be expected to contribute the EU's SST support framework,[38] particularly given that the Sentinel satellites will be primarily dedicated to earth observation rather than orbital surveillance and tracking. Nonetheless, it could be argued that by including this activity within the role of the programme's space segment, the EU is seeking synergy between its outer space programmes on the subject of outer space security.

Given the repeated references to climate change within the majority of themes and projects associated with Copernicus, it can be argued that the programme is designed to complement and enhance existing terrestrial measures associated with environmental security, making it an instrument of anticipatory security logic. Although the themes of

---

[38] For further discussion of the EU's SST support framework, see chapter 5 of this thesis.

atmospheric, land and marine monitoring, emergency management and security are relatively broad, the projects which have emerged through the FP7 are arguably a mix of both preemptive and preventive approaches to environmental security. On the one hand, a number of projects focus upon specific dangers, such as volcanoes and earthquakes, whilst at the other end of the scale many of the projects devoted to the monitoring of changes in land and marine environments are designed to identify possible future risks – relating for instance to forests and water quality – and inform efforts to mitigate them.

It has been argued above that the Copernicus programme does not provide services which could be deemed “essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions” (Council of the European Union, 2008a: L 345/77). Consequently, the programme does not appear to fulfil the requirements to be considered an ECI according to the Council of the European’s definition. However, the declaration by the European Commission (2011a) that “[s]pace infrastructure is critical infrastructure on which services that are essential to the smooth running of our societies and economies and to our citizens’ security depend” (p. 6) implies, as discussed earlier in this chapter, that all outer space infrastructures are deemed vital by the EC, thus establishing the criticality of, at the very least, the space segment of Copernicus. This position is continued in a 2013 Commission Staff Working Paper which, although not specifically mentioning Copernicus as it does Galileo, states that “[a]ny shutdown of even a part of space infrastructures could have significant consequences for the well-functioning of economic activities and our citizens’ safety and security, and would impair the provision of emergency services” (European Commission, 2013b: 13). Given the range of services and Horizon 2020-funded projects expected to depend upon data from Copernicus’ space segment, the argument can be made that the “provision of emergency services” in the event of a natural disaster may become reliant – if not dependent – upon Copernicus in the future. Furthermore, Copernicus will represent an autonomous European remote sensing capability, meaning that the EU will not have to depend upon other spacefaring actors for data to support its initiatives and policies in the areas of environmental security, emergency management and border security, whilst enabling Member States to have equal access to the services it provides. As discussed in chapter 2, independent outer space programmes enable the projection of European space power by promoting European economic, industrial and scientific capabilities. Given the remote sensing services Copernicus is expected to provide, the programme will arguably be integral to the EU’s desire for leadership in outer space affairs.

Although not necessarily fulfilling the requirements to be categorised as an ECI under the existing EU definition, Copernicus, like Galileo, will arguably be a future critical outer space infrastructure for the policy-multiplication opportunities it is expected to provide once completed, along with the blanket criticality imposed by the European Commission (2011a: 6) concerning outer space infrastructures.

3.8 Conclusion

As argued in chapter 2 of this thesis, outer space programmes are important contributors to the EU’s terrestrial and extra-terrestrial policy objectives. However, at the time of writing outer space infrastructures have not yet been included within the list of ECI sectors covered by the EPCIP (see Council of the European Union 2008a: L 345/81). Moreover, there is an emphasis on infrastructures to be located within the territorial boundaries of an EU Member State in order for them to be eligible for designation as ECIs (see Council of the European Union 2008a). Thus, despite the acknowledgement of their vital role within European societies and economies (European Commission, 2011a: 6; The European Parliament and the Council of the European Union, 2013: L 347/1; 2014b: L 122/44), extra-terrestrial infrastructures must be considered separate to their terrestrial counterparts in terms of security. While there is an established process for the identification and security of ECIs by EU Member States, the same does not exist, at least detailed in the public realm, concerning outer space assets. However, there is evidence to suggest that the EU’s position on European critical infrastructures is changing. The explicit inclusion of Galileo in a pilot programme concerned with inter- and intra-sectoral interdependencies arguably indicates a shift away from the narrow territorial boundaries which frame the existing ECI legislature.

The EU currently has two critical outer space infrastructures under development; the Galileo and Copernicus programmes. Through the provision of navigation and positioning signals to users worldwide in the areas of aviation, SAR, land and maritime transportation and fishing, Galileo may well become vital to a number of societal and economic functions for EU Member States. This is underlined by the EU expectations that once operational, Galileo will be integral to a number of inter- and intra-sectoral interdependencies (see European Commission, 2013b). Meanwhile, Copernicus promises to offer a number of services in the areas of land, marine and atmospheric monitoring, emergency management and security, with a general theme of climate change running across the aforementioned areas. Neither of these two programmes is offering completely novel services, although their introduction will augment existing GNSS services; Galileo may be the first European GNSS but the US GPS and Russian GLONASS are already operational, while Copernicus is arguably as much about the coordination of data from space-based and *in situ* sensors as it is about the provision of a new outer space infrastructure to support the proposed services. With regards to criticality, the navigation and positioning signals are arguably more vital to the societies they serve than the monitoring services provided by Copernicus. In particular, the bi-directional SAR capabilities that Galileo is expected to offer will be a significant improvement to existing communications between SAR teams and stranded persons. Nonetheless, once operational, both programmes will complement and augment existing capabilities in their respective fields, making them important components in a variety of societal and economic functions. They will, in other words, become integral to a number of inter- and intra-sectoral interdependencies (see European Commission, 2013b). Moreover, Galileo will ensure independence from the navigation and positioning signals provided by GPS, extending European autonomy in its terrestrial and outer space capabilities. If not then, according to the definition of the Council of the European Union (2008a: L 345/77), ECIs in themselves, the contributions that Galileo and Copernicus are expected to offer to EU societies and European space power once they are completed will make them critical outer space infrastructures in need of security.

The next two chapters summarise the most significant threats to outer space infrastructures and analyse the EU's response to these threats in terms of anticipatory security. Chapter 4 is focused upon what is termed 'intentional' threats, meaning dangers which result from the intentional actions of an actor, including the deliberate fragmentation of a space object or the increasing congestion at a number of popular orbital altitudes. The anti-satellite (ASAT) programmes of the US, Russia and China are discussed, and the chapter concludes by analysing the EU's main contribution thus far to diplomatic endeavours concerning outer space: the draft International Code of Conduct for Outer Space Activities. The subsequent chapter deals with environmental hazards to outer space infrastructures, including space weather and space debris, and analyses the EU's efforts to develop a European SSA.

4 Intentional man-made threats to the security of critical outer space infrastructures

As discussed in chapter 3, outer space assets and the services they provide are considered critical infrastructures by the European Union (EU), even if they are not yet afforded the same guarantees regarding identification and security as terrestrial European Critical Infrastructures (ECIs). Nonetheless, these extra-terrestrial infrastructures must be secured against a wide range of risks and threats, which will be the subject of the next two chapters. This chapter will introduce and discuss what can be termed ‘intentional interference’ against outer space infrastructures; in other words, deliberate actions by a party with the objective of interfering with the operations of a satellite or satellite constellation. The intentional interference with satellites is particularly strenuous on the EU’s approach to outer space affairs, as it attempts to maintain a largely civilian space programme. Although some of its programmes do have potential military applications, military space projects are largely undertaken by the European Defence Agency (EDA) and Member States rather than the EU or the European Space Agency (ESA). Environmental risks and dangers – the largely unintentional interference – are the focus of chapter 5.

This chapter begins by detailing the divide between the militarisation and the weaponisation of space, two notions which are “sometimes blurred, intentionally or unintentionally” (Johnson-Freese, 2007: 2). It then offers a brief history of the development of anti-satellite (ASAT) systems and technologies as background to the on-going debates over the weaponisation of outer space. As the US has undertaken the most research into ASAT technologies, the military doctrine underpinning its space policies is also discussed. The chapter then analyses the extent to which on-going efforts to prevent intentional man-made threats to outer space infrastructures, and in particular the draft International Code of Conduct for Outer Space Activities championed by the EU, are advocating sustainability and logics of anticipatory security.

Terrestrial warfare takes place on land, at sea and in the air. It takes place beneath ground through the use of tunnels for both offensive and defensive operations and in the depths of the seas and oceans through the use of submarines and sea mines. It is not particularly surprising that military strategists would look to outer space as an opportunity for furthering operational capabilities, and the costs associated with developing, launching and operating satellites meant that the early years of the exploitation and exploration of near-Earth space were limited to projects afforded government or military funding. In the early 21st Century, there remains a significant military presence in near-Earth space with satellites dedicated to a number of tasks, including transmitting secure communications, providing surveillance capabilities and early warning of missile launches. As yet however, public knowledge is that there are no active weapons systems deployed in outer space (Wright *et al.*, 2005).

4.1 The militarisation and weaponisation of outer space

There has been substantial scholarly debate over the terms militarisation and weaponisation with respect to the domain of outer space. The distinction between these two terms must be emphasised: militarisation refers to the use of man-made assets orbiting the Earth for passive military purposes, for instance force multiplication, surveillance and treaty verification. Weaponisation, on the other hand, implies the deployment of systems in outer space that could be used to strike targets within the Earth's atmosphere or in the domain of outer space itself. That near-Earth space is militarised is widely accepted amongst academic scholarship (see Aldridge, 1987; O'Hanlon, 2004; Sheehan, 2007: 94), however there is continued evidence of determination on behalf of the US, if not others, to weaponise the domain.

The military applications of satellites have been at the forefront of political rhetoric since the launch of Sputnik in 1957, an event which, Sheehan (2007) argues, infused the US space programme with an energy that had not been present beforehand, as the USSR was seen has having achieved technological superiority in matters pertaining to outer space (p. 40). The 1955 US National Security Council (NSC) report NSC 5520 – which officially recommended the development of a "small scientific satellite" (National Security Council, 1955: 6) – includes numerous references to the intelligence and military benefits of launching a satellite into orbit. Although the NSC report acknowledges that a small satellite will not be able to carry surveillance sensors "and therefore will have no direct intelligence potential, it does represent a technological step toward the achievement of the large surveillance satellite" (National Security Council, 1955: 2-3). Equally, in the technical annex to the report, it is stated that "[a]nti-missile missile [*sic*] research will be aided by the experience gained in finding and tracking artificial satellites" (National Security Council, 1955: 8). It is apparent then that even while the US space programme was in its infancy, the intelligence and military communities recognised the potential of Earth-orbiting satellites for their respective fields of work. The focus, at this time, appears to have been on what can be accounted for as the militarisation of outer space, however the development of any launch vehicle with the capability of delivering a payload into orbit could easily have other military applications, as these vehicles share a lot in common with Inter-Continental Ballistic Missiles (ICBMs) and indeed many early launch vehicles were adaptations or combinations of existing rocket designs.

Nowadays near-Earth space is host to a large number of satellites engaging in a multitude of operations, many of which have military applications. A substantial proportion – Johnson-Freese (2006: 131) suggests 95% of satellites and their services – can have both military and civilian applications; these technologies are termed ‘dual-use’. To take one example, meteorological satellites offer civilian populations information about weather in the coming days or weeks so that they can plan for extreme weather events or simply know whether to take an umbrella to work on a particular day. These meteorological satellites also provide a stream of data to scientific research institutions studying long- and short-term weather as well as other atmospheric phenomena. However, the data from those same satellites can be used by militaries for a number of purposes, including the coordination of ground and air operations. These meteorological satellites and services could thus be considered critical infrastructures for both civilian and military spheres.

From an academic standpoint, Johnson-Freese (2007) contends that there has been little debate over the weaponisation of outer space, though this is not to say the issue has not been scrutinised. There is, within the literature concerned with the weaponisation of outer space, a divide between those who believe weaponisation must be prevented – the ‘sanctuary’ approach proposed by Ziegler (1999) – and those who believe weaponisation to be a necessity for national security (Dolman, 2002; Kleinberg, 2007; A. Steinberg, 2012). Much of the academic debate regarding the weaponisation of outer space that is written in English originates from the US, though some notable exceptions include Sachdeva’s (2009) discussion of the legality of ‘space mines’, contributions in Bormann and Sheehan’s (2012) *Securing Outer Space*, Sheehan’s (2007) monograph titled *The International Politics of Outer Space* and People’s (2008; 2010b; 2011) articles on securitisation and the supposed inevitability of outer space becoming weaponised. From a scientific rather than

International Relations perspective, and although not explicitly calling for outer space to remain a sanctuary from active weapons, Wright *et al.* (2005) critically evaluate the physics and astrophysics behind space weapons, arguing that current technological capabilities would render them costly and inefficient.

O'Hanlon (2004) argues in favour of the US looking towards the future weaponisation of the domain but recommends that in the short-term it should avoid developing ASATs, as he believes that the first country to do so will spark an arms race (p. 24). His argument is a representation of the security dilemma, with states attempting to develop an offensive defensive weapon (ASATs) for their own security and in doing so threatening other space users, thus leading to them developing weapons of their own. O'Hanlon, like Dolman (2002), believes the US must maintain its dominance in outer space and is of the opinion that the weaponisation will be an inevitable part of this continued primacy. Dolman, though, goes further with his theory of adaptation of classical geopolitics under the name 'Astropolitik'. At the forefront of Astropolitik is the concept of space control, whereby a state can achieve primacy in terrestrial politics through the domination of near-Earth space, and in particular through the seizure of specific 'choke-points', namely the Hohmann transfer orbits, the geostationary belt, the Lagrange libration points and Lower Earth Orbit (LEO) (Dolman, 2002: 71-76). This approach takes outer space to be "the ultimate high ground" (Dolman, 2002: 151), providing unrivalled strategic advantage to whoever 'controls' it, which, in Dolman's opinion, should be the US because of its emphasis on morality as a core value.

However, while Astropolitik may only be one possible direction for US space policy, it is nevertheless a potentially dangerous line of thinking for two reasons. Firstly, the notion of space control advocates the use of ASAT weapons if required to establish and maintain dominance in outer space, completely disregarding the environmental implications this would have for the domain, despite the historical experiences of orbital nuclear weapons-testing (Moltz, 2008: 51-56). Depending on its orbit, pieces of debris can remain in outer space for decades, centuries and even millennia (National Aeronautics and Space Administration, 2009: 22-23; O'Hanlon, 2004: 42; Wright, 2007; 2009), making it an issue worthy of concern, especially considering that the use of physical ASAT weapons can lead to the generation of large amounts of long-lasting debris, as shown by the Chinese ASAT test of January 2007 (Wright, 2007; 2009).

Secondly, the perception of outer space as "the ultimate high ground" (Dolman, 2002: 151) transforms space into a strategic resource and an object of military desire.[39] It supports the notion that near-Earth space, or Terran space as Dolman (2002: 69) calls it, is an extension of the planetary sphere. Activities within this region are imagined as being, for all intent and purpose, as taking place within the confines of the Earth. This close association between the Earth and near-Earth space is arguably a dangerous one, as it risks providing justification for the extension of military practices normalised on Earth. There is agreement that while outer space is already militarised (see Dolman, 2002; Grondin, 2012; O'Hanlon, 2004; Sheehan, 2007), it is not yet weaponised. It is important to note though that this strategic approach to outer space, combined with the idea of space control, could well have implications for the concept of sovereignty and the benefits it provides to states on Earth (Duvall and Havercroft, 2008).

Before any thorough discussion of the militarisation and weaponisation of outer space can occur, the scope of both terms needs to be further established. For the purpose of this thesis, militarisation shall be deemed to include activities with both military and dual-use applications, including but not limited to: surveillance conducted by dedicated

---

[39] For example, the Cold War 'space race' reflected the perceived strategic importance of outer space. For more on this, see Cadbury (2005), Dolman (2002), O'Hanlon (2004) and Sheehan (2007).

military-operated satellites, the transmission of military and government communications through dedicated or commercial satellite networks and the provision of navigation and positioning signals used by military forces for movement or ordnance targeting. The militarisation of outer space is a complex issue given the plethora of systems with dual-use capabilities; for instance a commercial remote sensing satellite may in theory not be a military system, but if its operators were to sell images from that satellite to governments which use them for military purposes, the output arguably then becomes military in nature. In addition, although ballistic missiles may have trajectories taking them briefly into 'outer space', this thesis adopts a similar stance to Krepon *et al*. (2011) insofar as these systems are considered to be "ground-based weapons aimed at ground-based targets, rather than being weapons based in space or aimed at space-based targets" (p. 3).

In comparison, the use of the term weaponisation in this thesis is at first glance fairly simple, in that it relates solely to the deployment of weapons systems in outer space. However, like the complexity surrounding militarised satellite systems, there is, at the time of writing, no widely agreed definition of a space weapon (Peoples, 2011: 78). The problem is exacerbated by the fact that although terrestrial weapons systems such as ASATs or jamming equipment would likely be important features of a hypothetical future space war, they are not inherently space weapons, situated as they are within the confines of the Earth's atmosphere. Furthermore, some academics, such as Moltz (2008: 43), have chosen to exclude systems which impose only temporary effects on satellite operations; an approach which is arguably problematic as it ignores equipment capable of jamming and spoofing signals. Although these systems may only interfere with the operations of a satellite, rather than damage it, their capability to disrupt the provision of services means that they should not be ignored as potential weapons.

For the purpose of this thesis, space-based ASAT weapons will be considered to be any dedicated system based in near-Earth space used intentionally to interfere with the structural integrity or operations of spacecraft – active or otherwise – without the permission of the spacecraft's owner. The intention here is to incorporate all forms of intentional interference originating from outside the Earth's atmosphere which may be undertaken against man-made objects orbiting the Earth. As per the demarcation between airspace and outer discussed in chapter 1, this definition includes any weapons systems located above the Kármán line. Although this definition is thus relatively wide in its scope, it includes a number of systems which may be excluded from existing definitions elsewhere. It should also be re-emphasised that this definition does not include terrestrially-based weapon systems. The reason for this is that although the systems they will contribute to a hypothetical war in outer space, the location within the confines of the Earth's atmosphere means that in this thesis, they are separated from those systems based in outer space itself. It must be emphasised that this does not ignore the threat posed by terrestrial ASAT systems, only that they are considered separately from their space-based equivalents. The reason for this differentiation is that a number of Earth-based ASAT weapons could be considered dual-use, insofar as with some adaptation they can be directed at satellites or missiles; the US Ballistic Missile Defence (BMD) system used to destroy USA-193 in 2008 is a case in point. Moreover, as discussed in more detail below, terrestrial ASAT systems have been successfully tested, while at the time of writing there is no information in the public domain indicating the existence of operational or demonstration space-based weapons systems. Separating terrestrial ASAT systems and space-based ones therefore allows a discussion of existing threats to the space segments of outer space infrastructures whilst avoiding digressions into fantasy. For the purposes of this thesis then, terrestrial ASAT systems refer to any systems based, launched or deployed from below the Kármán line that are used to intentionally interfere with the structural integrity or operations of spacecraft – active or otherwise – without the permission of the spacecraft's owner. With regards to the jamming and spoofing of satellite signals, historical examples of these have originated from equipment based on Earth and thus, according to the definition outlined above, they would not be considered space weapons. However, should future systems capable of jamming or spoofing signals be deployed on satellites, then those satellites would be deemed to be space weapons as soon as the equipment were used.

The concept of militarisation in outer space is distinct from how the term is used with regards to terrestrial contexts, where it is often associated with militarism (see Kohn, 2009). The wider terrestrial use of militarisation extends to studies in a number of disciplines, including but not limited to the sociology of video games (see Martino, 2012), social psychology (see Orr, 2004) and gender studies (see Cock, 1989). The narrow focus of militarisation in this thesis and indeed much of the academic literature on outer space arguably originates in the desire to differentiate between the use of satellites for passive military purposes – in other words force multiplication – and the deployment of active weapons into orbit.

The divide between militarisation and weaponisation may appear on the surface to be unnecessary as the latter, if it occurs, would be part of a wider militarisation of outer space. However, separating activities as being associated with militarisation or weaponisation is arguably integral to both sides of the debate on space weapons; on the one hand, the division normalises 'good practice' in outer space, where the domain is maintained free from aggressive military operations, distinct as it were from the ground, sea and air theatres of Earth (see Ziegler, 1999). Those in favour of weaponisation however use the term almost as an ambition yet to be met. Although the deployment of space weapons has been described as necessary for the protection of an actor's space assets (see Dolman, 2006; 2010; A. Steinberg, 2012), it has not yet taken place. Thus for advocates of weaponisation, the term represents an objective towards which they continue to lobby.

This chapter will continue by discussing ASAT systems – which have a history of successful testing – before turning to other forms of intentional dangers to outer space assets. It will then explore the existing legal regimes on outer space activities, before concluding with an analysis of European efforts to prevent the weaponisation of outer space through international diplomatic initiatives.

4.1.1 ASAT weapons

ASAT weapons have been under development by spacefaring entities since very early on in the history of human exploration and exploitation of outer space. Given that the human species' first concerted and successful efforts to travel beyond the confines of the Earth's atmosphere took place within the context of the Cold War, this is arguably unsurprising. The first work on ASAT systems by the US and the USSR were during the mid- to late 1950s not long after the launch of Sputnik, indicative of an acknowledgement of the vertical vulnerability introduced by orbiting satellites. This manifestation of vertical vulnerability is not unlike the fears of the British populace in the early 20th Century, when there was a series of sightings of vast airships over the United Kingdom in 1909, which, although later proven to be imaginary, nevertheless "expressed and fomented Britain's paranoia that its island security was soon to be at an end" (Adey, 2010: 55). It is also representative of what Butler (2001) terms 'technogeopolitics' – "the recursive relationship between technology and geopolitics" (p. 637) – insofar as the US and the USSR, threatened by the possibility of operational weapons platforms orbiting in a frictionless vacuum above their respective territories, felt the need to initiate research and development of counter-measures before such weapons platforms even existed.

It must be emphasised that the testing and deployment of ASATs does not necessarily infer the weaponisation of outer space. With the exception of the US Brilliant Pebbles programme – which was cancelled in 1993 – it would appear that no space-based systems with a potential ASAT capability have yet been developed. All the ASAT systems about which information is available in the public sphere are exclusively ground-based. Even the Soviet co-orbital ASAT – which destroyed satellites by manoeuvring nearby before detonating explosives destroying both itself and its target – needed to be launched from the Earth only hours before any planned intercept. Nonetheless, there remains a possibility that space-based ASATs will be developed in the future. Moreover, the decision to pursue the development of ASAT systems is arguably indicative of the stance an entity takes towards near-Earth space.

There are three main types of ASATs: Isotropic Nuclear Weapons (INW), Kinetic-Energy Weapons (KEW) – otherwise known as kinetic-kill weapons – and Directed-Energy Weapons (DEW) (Johnson-Freese, 2009: 9). Although early ASAT systems, particularly in the US, used INWs, contemporary systems, as far as information available in the public domain indicates, employ KEWs or DEWs. It is outside the scope of this thesis to provide a detailed account of all ASAT developments since the 1950s, however some significant systems and events will be charted below in order to provide background.

4.1.1.1 US ASAT programmes

Although there was some reluctance within US political circles during the 1950s about the need for orbital weapons systems, military commanders and planners were more open to the idea (Sheehan, 2007). Early US ASAT efforts revolved around the use of nuclear armaments to counter possible orbital nuclear weapons platforms (Globalsecurity.org, 2011a). The first US ASAT test was in 1959 as part of project Bold Orion and involved an Air-Launched Ballistic Missile (ALBM) targeting a US satellite, although no impact took place. There were only two tests of the Bold Orion ALBM in its ASAT format, although in the 1960s, the US Air Force (USAAF) maintained an operational ASAT capability through ground-based Thor missiles (Aldridge, 1987). The first successful US ASAT test took place in 1963 using the US Army's Nike-Zeus rocket, following the system's ineffectiveness as an Anti-Ballistic Missile (ABM) system (Globalsecurity.org, 2011a).

The Thor nuclear ASAT arsenal was withdrawn from service in 1976, although it has been retained in a decommissioned state, with the capability to be returned to operational service within six months should the US choose to resume above-ground nuclear testing should the Limited Test Ban Treaty be abandoned (Globalsecurity.org, 2011a). The end of the Thor system did not spell the end of US ASAT projects though. In 1982, the Reagan administration issued a revised national space policy, replacing a previous policy document published in 1981. Sheehan (2007) contends that the revised document "called for development of an operational anti-satellite system" (p. 97), however no such statement appears to exist within the declassified version (see White House, 2010a).[40] Nonetheless, in 1985, the US tested the first Air-Launched Miniature Vehicle (ALMV) ASAT, conducting a successful interception with the Solwind P78-1 meteorological satellite on September 13th of that year. The ALMV employed a kinetic-kill Miniature Homing Vehicle (MHV) launched from modified F-15 (see figure 4.1), which afforded it mobility ground-based ASATs could not match. The project continued despite a

---

[40] It must be noted though that some sentences and paragraphs remain redacted as part of the declassification process.

Congressional ban on ASAT testing issued in late 1985 (Grego, 2012a; Sheehan, 2007) but it was eventually abandoned in 1988 after increasing costs and technical problems (Dvorkin, 2010: 35).

Figure 4.1 The ALMV launched against the Solwind P78-1 satellite in September 1985 (Air Force Space Command Public Affairs, 2012) – The image has been excluded from this electronic version of the thesis to ensure compliance with copyright legislation.

The Congressional ban on ASAT testing ended in 1988 and the US military began research into DEW ASATs (Grego, 2012a: 5-6). Although kinetic-kill weapons have a longer range than laser and microwave weapons and are not affected by poor weather, Grego (2012a) comments that “they are also likely to produce significant space debris and are easily linked to the source of the attack”, while “ASAT weapons based on **directed electromagnetic energy** (such as lasers or high-powered microwaves) […] produce a great deal less debris and may allow for a cover attack (or at least delayed identification of the attacker)” (p. 6, original emphasis). The two forms of ASAT also offer advantages and disadvantages depending on the interference intended; kinetic-kill systems destroy satellites, whilst, depending on the intensity of the beam, laser and microwave weapons can temporarily or permanently interfere with a satellite’s sensors, or destroy the target (Johnson-Freese, 2009: 9). The move towards directed electromagnetic energy ASATs included the development of the Mid-Infrared Advanced Chemical Laser (MIRACL), based at the White Sands Missile Range in New Mexico (Dvorkin, 2010). The system was temporarily banned by Congress between 1991 and 1996 after it was confirmed that the Soviet/Russian version was of little or no threat to US satellites (Webb, 2012). After its use was allowed once again, MIRACL was successfully tested in October 1997, when it ‘illuminated’ a satellite orbiting at 420km altitude (Grego, 2012a: 7). The results of the test are confidential (Grego, 2012a: 7) but Dvorkin (2010) suggests that the test indicated that the system could cause damage to a satellite’s solar panels and optical sensors (p. 36).

Another DEW system developed by the US is the Airborne Laser (ABL), which involved a Chemical Oxygen-Iodine Laser (COIL) housed within a modified Boeing 747-400F capable of destroying missiles and either destroying or blinding satellites (Webb, 2012: 29), making it both useful as part of the US BMD system and as a potential ASAT system. Although the ABL successfully destroyed two target missiles in 2010, funding was cut in 2011, effectively ending the project (Butler, 2011). Additionally, Webb (2012) notes that plans for a Space-Based Laser (SBL) using a chemical laser similar to MIRACL and COIL appear to have fallen by the wayside, with efforts directed towards ground-based lasers directed by mirrors mounted on aircraft or towards the less powerful but smaller and longer-lasting Solid State Lasers (SSLs) (p. 29).

On the 20th February 2008, the US launched an ASAT against USA-193, a National Reconnaissance Office (NRO) satellite launched in 2006 but which had malfunctioned soon afterwards, leaving it in a deteriorating orbit. Although the covert nature of the satellite’s planned operations meant that its orbital deterioration was not publically announced until January 2008, amateur observers noted the malfunction and provided data which enabled Pardini and Anselmo (2009) to calculate preliminary predictions for USA-193's re-entry. The destruction of the satellite was publically justified by fears that the satellite's fuel tank, containing the carcinogenic and toxic hydrazine fuel, might survive re-entry into the atmosphere and land near a populated area (Shanker, 2008). The satellite was destroyed by a kinetic-kill SM-3 missile launched from the USS *Lake Eerie* which collided with its target at an altitude of around 133 miles (214km) (Mineiro, 2008: 349-350), resulting in a "substantial debris cloud" (Pardini and Anselmo, 2009: 792), although very little of said debris was long-lasting; by June 2008, only two catalogued space debris objects (debris larger than 10cm) remained in orbit (Pardini and Anselmo, 2009: 794). The event marked the first intentional destruction of a satellite by the US since the 1980s and provoked concern from Russia and China (Johnson-Freese, 2009), despite the latter having conducted an ASAT test a year earlier which had created a significant amount of debris in LEO. One of the areas of concern was that the SM-3 missile employed is part of the US BMD system, leading to suggestions that other SM-3 missiles could be modified to act as offensive, as well as defensive, weapons (Grego, 2012a: 12).

4.1.1.1.1 US military doctrine on outer space

It is worth taking a brief deviation into US military doctrine – "the structured thinking about military operations that guides the training, equipping and employment of military forces" (Sheehan, 2007: 110) – as it offer insights into the development of how military commanders and planners conceive conflict in and through the domain of outer space. Although as mentioned above, development of ASAT systems began very soon after Sputnik's first successful orbit around the Earth, attempts to formulate a comprehensive doctrine for their effective use in conflict did not emerge until the 1970s.[41] There was a doctrinal evolution through the 1970s and 1980s, with the first space-specific doctrinal document published in 1977. During this time, the overarching approach of the US military to outer space was split "between a desire to preserve space as a peaceful sanctuary and a recognition of its potential as a theatre of military operations" (Sheehan, 2007: 110).

Outer space and, specifically, near-Earth orbital space offer a different set of advantages and vulnerabilities for military commanders and planners. US military doctrine advises its Joint Forces Commanders (JCFs) that they must be aware of these advantages and vulnerabilities, warning that:

> Commanders should consider the possibility of hostile actions from state and non-state actors intended to deny friendly forces access to, or use of, space capabilities while developing strategic estimates, plans, and other documents and planning future operations and activities. They also should anticipate the proliferation and increasing sophistication of space capabilities and products with military utility that could be used by any adversary for hostile purposes. Potential adversaries no longer have to develop large infrastructures to obtain or interfere with space capabilities. Today, many capabilities can be easily purchased (Joint Chiefs of Staff, 2013b: I-2).

It is apparent from this that the US military still perceives outer space to be a potential battleground, or at least a domain in which assets can be deployed with the capability to affect the conduct of terrestrial military operations. In other words, the US military is

---

[41] See Sheehan (2007: 109-120) for a detailed account of the evolution of US military doctrine on space warfare.

acknowledging the militarisation of outer space and warning against the future weaponisation of the domain, or at least the possible use of ASATs by adversaries.

Contemporary US military doctrine on outer space involves five forms of operations: space situational awareness, space force enhancement, space support, space force application and space control (Joint Chiefs of Staff, 2013b: x-xi; United States Air Force, 2011: 45). According to the 2013 Joint Publication 3-14 (JP3-14) document published by the Joint Chiefs of Staff, space force enhancement involves "increasing the combat potential of […a] force, enhancing operational awareness, and providing critical joint force support" (Joint Chiefs of Staff, 2013b: II-4). It arguably incorporates all forms of space-based applications which could be considered dual-use, including meteorology, communications and navigation, as well as applications traditionally perceived as located within the military sphere, such as surveillance, missile warning capabilities and Signals Intelligence (SIGINT). All these missions are of critical importance to military operations; meteorological information allows commanders to plan operations, both on the ground and in the air, whilst navigation services enable accurate transportation and the use of so-called 'smart' weapons[42] in combat. In addition, Joint Direct Attack Munitions (JDAMs) can be attached to non-guided munitions, transforming them into 'smart' weapons. Military-specific force enhancement technologies, such as military surveillance satellites, offer high-resolution imagery of selected areas of the Earth's surface. Although these satellites can only view a certain area at one time, their orbital paths cover the entire globe, meaning that features or locations of interest fall within their coverage around twice a day. Missile warning capabilities are fairly straightforward, insofar as satellites dedicated to that task report any events within the Earth's atmosphere which display similar characteristics to a rocket or missile launch. Finally, SIGINT satellites intercept electronic transmissions, both

---

[42] These are munitions guided to their target by GNSS signals.

linguistic and non-linguistic. As Johnson-Freese (2007) notes, the interception of radar signals can be as important as the interception of transmissions carrying written or voiced commands, as the former can offer indications as to an opponent's location and force strength (pp. 90-91).

Space support, meanwhile, is concerned with the logistical side of space affairs, including 'spacelift operations' – "the ability to deliver satellites, payloads, and material into space" (Joint Chiefs of Staff, 2013b: II-6) – satellite operations – "operations conducted to maneuver [*sic*], configure, operate and sustain on-orbit assets" (Joint Chiefs of Staff, 2013b: II-7) – and reconstitution of space forces – "plans and operations for replenishing lost or diminished space capabilities" (Joint Chiefs of Staff, 2013b: II-8). Although, at first glance, this area could easily be considered the least important for military operations as it does not contribute directly to them, space support missions are arguably the complete opposite. The capability to launch satellites into orbit cost-effectively and reliably is critical to a successful outer space programme, be it civilian or military. Indeed, unlike other aspects of rocketry, such as the development of ballistic missiles for military purposes, launchers for space payloads must have a very high degree of reliability. While the occasional failure of a ballistic missile could cost a few thousand dollars or pounds, the failure of a launcher could lead to costs in the millions because of the price of producing replacement payloads and loss of profits (Johnson-Freese, 2007). Finally, space support capabilities may well become the most critical in the event of a conflict involving the use of ASAT systems, as the continued access to space assets and the services they provide will be crucial.

Space control is one the two most controversial mission types, as it "provides freedom of action in space for friendly forces, and when necessary, defeats adversary efforts that interfere with or attack US or allied space systems and negates adversary space capabilities" (Joint Chiefs of Staff, 2013b: II-8). The use of the term 'adversary' is arguably ambiguous, with little indication as to whether an adversary would have to be an entity actively engaged in military conflict the US. The possibility remains that the space control doctrine could advocate the use of offensive weapons preemptively against an entity the US fears could become an adversary in the future. Nonetheless, the inclusion of both defensive and offensive spheres to space control is arguably more restrained than the space control proposed by Dolman (2002) in his theory of Astropolitik, which centres on the US seizing near-Earth space to ensure its dominance. Indeed, the 2013 JP3-14 doctrinal document mentions a number of non-military means, including the "diplomatic, informational, […] and economic measures (Joint Chiefs of Staff, 2013b: II-8), which can be employed to prevent the use of systems which could limit the US or its allies the freedom of action in outer space. The inclusion of 'prevention' as an integral aspect of space control represents a shift from the definition of space control present in the US Air Force Doctrine Document 1 of 1997, in which space control is defined as "[a]chieved through offensive and defensive counterspace carried out to gain and maintain control of activities conducted in or through the space environment (United States Air Force, 1997: 84-85). Additionally, although prevention is included in the 2002 JP3-14 document, its description is quite ambiguous, with "military, diplomatic, political, and economic measures" available for use "as appropriate" (see Joint Chiefs of Staff, 2002: IV-7). Of course, systems designed to negate an adversary's space assets or capabilities are also discussed, as the US has actively researched such systems in the past. Perhaps surprisingly, a capability described as vital to space control in the 2013 JP3-14 document is Space Situational Awareness (SSA) (Joint Chiefs of Staff, 2013b: II-1). Although SSA is regularly referred to in relation to the monitoring and tracking of space debris (see chapter 5 of this thesis) rather than military operations, the JP3-14 document makes it clear that increased knowledge of objects orbiting the Earth and space weather phenomena are at a similar level of importance to the knowledge of satellite manoeuvres (p. II-1-II-3). The JP3-14 document also considers terrestrial reconnaissance by space-based or airborne assets as part of SSA, presumably because it also includes an entity's ground segments (for example launch locations and control buildings) as part of its space capability (p. II-1). Although this is a logical step from a military standpoint, it is notable that the European SSA, run purely as a civilian programme, includes only the surveillance and tracking of space objects. It could be argued that by expanding the space control mission from being purely about the negation of an adversary's space capabilities to the overall protection of its space assets, the US has moved away from space 'control' to a more generic form of space 'defence'. At the very least, it is a far cry from the belligerent space dominance advocated by Dolman (2002; 2006; 2010).

The final mission defined within the 2013 JP3-14 document is space force application. Details on this mission are limited because the document does not provide much information, stating that:

> Space force application is combat operations in, through, and from space to influence the course and outcome of conflict by holding terrestrial targets at risk. The space force application mission area includes ballistic missile defense and force projection capabilities such as intercontinental ballistic missiles. This mission area is incorporated into national space policy as well. Specific responsibilities can be found in DODI [Department of Defense Instruction] S-3100.13, *Space Force Application.* (Joint Chiefs of Staff, 2013b: II-9-II-10, original emphasis).

Following attempts to access DODI S-3100.13, it appears that it remains a confidential document currently not available for public access, so the specifics of space force application contained within the instruction cannot be commented on. The *Department of Defense Dictionary of Military and Associated Terms* repeats the definition included within the JP3-14 document insofar as space force application refers to “combat operations in, through, and from space to influence the course and outcome of conflict by holding terrestrial targets at risk.” (Joint Chiefs of Staff, 2013a: 258). Consequently, it appears that space force application includes the targeting of ground-based and sub-orbital targets using technology which is launched from or passes through outer space, making it the only mission area which explicitly calls for the development of space-based weapons systems.

Although all four of the aforementioned missions are incorporated within US military doctrine, only one of them, space force application, may include the development of space-based weapons systems. Space control, whilst controversial, could arguably be achieved solely by the use of ground-based ASAT or BMD systems, although space-based systems such as Brilliant Pebbles have been developed even though as yet it is not known that any are operational.

4.1.1.2 Russian ASAT programmes

The USSR first maintained a potential ASAT capability in the 1960s, when it deployed a ring of nuclear ICBMs around Moscow to act as an ABM system. Grego (2012a: 2) and Webb (2012: 28) contend that these ICBMs, although ostensibly a defensive measure, could easily have been adapted to act as a crude ASAT system as an exo-atmospheric nuclear detonation would indiscriminately destroy any nearby satellites, as well as substantially increasing the radiation levels in LEO.

The main Soviet ASAT programme, development of which began in the 1960s, was a co-orbital weapon, whereby an interceptor with a payload of explosives would be launched and manoeuvred to near a satellite, at which point the payload would be detonated, destroying both the ASAT interceptor and its target (Grego, 2012a: 3; Sheehan, 2007: 103). The co-orbital interceptor was designed to approach its target within one or two orbits – a time period of between one and a half to three hours (Grego, 2012a: 3) – before destroying it with shrapnel from the detonated explosive payload. Testing of the co-orbital ASAT system began in 1963 – with the first successful mission taking place in 1968 (Dvorkin, 2010: 32) – and continued until 1973. During this time, seven tests were conducted, five of which involved confirmed detonations (Grego, 2012a: 3), indicating that the system was effective from 230km to 1000km in altitude (Dvorkin, 2010: 32). Testing resumed in 1978 and lasted until 1982, when a moratorium was issued on ASAT testing, providing no other state deployed an operational ASAT system in outer space (Webb, 2012: 28). The system was eventually withdrawn from service, on the orders of then Russian President Boris Yeltsin, in 1993 (Dvorkin, 2010: 32). The Soviet co-orbital ASAT system was capable of destroying satellites, that much was proved through its years of testing. However, it was limited by the fact it could only engage a satellite passing over its launch site, meaning that a target was only within range twice a day (Grego, 2012a: 3; Flynn, 1986: 28).

In 2009, it was reported that the Russian Federation was resuming its ASAT programme as part of a plan to develop a comprehensive air and space defence capability by the year 2020 (Kramnik, 2009). A year later, a Russian military officer claimed in an interview that Russia had begun development of an ASAT system “that can destroy potential targets in space” (Sigalov, E. quoted in: RIA Novosti, 2010). Kramnik (2009) suggests that the ASAT system under development is based upon an air-launched missile system – named KONTACT – originally developed during the 1980s employing a MiG-31 Foxhound to launch a KEW towards a target satellite (see Dvorkin, 2010: 32). This system bears similarities to the US programme mentioned above, which involved an ALMV launched from an F-15. Unlike Russia's co-orbital ASAT programme, there is no definitive evidence of the KONTACT system having been successfully tested, however it offers a much more flexible ASAT capability than its predecessor, which may explain the decision to update it as part of the renewed Russian efforts for space defence.

Although, at this time, few details exist of any new system other than reports on the website of the Russian news outlet RIA Novosti, the resumption of ASAT development by Russia would mark a significant change in its approach to outer space affairs, not least because of its efforts on the international stage to promote the proposed Treaty on Prevention of the Placement of Weapons in Outer Space and of the Threat or Use of Force against Outer Space Objects (PPWT). This treaty was first proposed by the People's Republic of China (PRC) and the Russian Federation in 2008 as a legal instrument for the prevention of the weaponisation of outer space. Although the PPWT will be discussed later, suffice to say for the moment that, as its name suggests, it is particularly concerned with the use of ASAT weapons against all objects in the domain of outer space. It is perhaps telling then of the pessimism present within Russian political thought that alongside these diplomatic efforts to prevent the weaponisation of outer space, the Russian Federation is actively developing an ASAT capability, albeit allegedly only for defensive purposes (see RIA Novosti, 2009). Indeed, Colonel General Zelin is quoted as predicting that "By 2030…foreign countries, particularly the United States, will be able to deliver coordinated high-precision strikes from air and space against any target on the whole territory of Russia" (Zelin, A. quoted in: Ria Novosti, 2009). The plausibility of these predictions is arguably debatable however, as discussed above, the US is certainly proceeding in a doctrinal direction which could well lead to the future development of systems capable of space-based force application; or in other words, space-to-Earth weapons. It must be emphasised though that no matter what the justification is for the resumption of ASAT development by the Russian Federation, such systems are not purely defensive. Should Russia succeed with the deployment of an ASAT system in the coming decades, it will inevitably have an offensive, as well defensive, capability.

4.1.1.3 Chinese ASAT programmes

In 2007, the PRC became the third country, after the US and the USSR, to successfully destroy an orbiting satellite. On the 11th January of that year, it launched a direct-ascent kinetic-kill missile against the Fen-Yung 1C (FY-1C) weather satellite, impacting at an altitude of around 530 miles (853km) (Kan, 2007: 1), although there was no public confirmation of the test by the PRC until the 23rd January (Mineiro, 2008: 341). The test received criticism, not least because of the extensive debris field that it generated (see Webb, 2012: 29), and was the first intentional destruction of a satellite since the US launched the ALMV against the Solwind P78-1 satellite in 1985 (Kan, 2007: 2).

The Chinese ASAT programme appears to have been first reported to Congress by the US Secretary of Defense in 1998 (Kan, 2007: 2), although Grego (2012a) suggests that a kinetic-kill ASAT system had been under development since the 1980s (p. 13). Two tests were conducted prior to the destruction of FY-1C: one in 2005 and one in 2006 (Gordon and Cloud, 2007). Although US officials were aware of plans for a third kinetic-kill ASAT test (Milowicki and Johnson-Freese, 2008: 4), a decision was made not to ask the Chinese to forego it as it was “concluded that China was unlikely to cancel the test and that there were few good options to punish China if they ignored an American warning to hold off” (Gordon and Cloud, 2007). In addition to the limited diplomatic options, “American intelligence agencies were loath to let the Chinese know they were aware of the state of their preparations" (Gordon and Cloud, 2007).

The destruction of FY-1C generated 3000 catalogued pieces of space debris, that is to say, 3000 objects larger than 10cm in size. Together with the 2000 pieces of catalogued debris created by the collision between the Iridium-33 and Kosmos-2251 satellites in 2009, the debris cloud from 2007 Chinese ASAT makes up over a third of the current catalogued debris in LEO (Anonymous, 2012c), with 90% of the original clouds still in orbit (NASA Orbital Debris Program Office, 2012b: 2). Moreover, because the altitude of impact was much higher than that which destroyed USA-193 in 2008, the debris generated from the Chinese test has a much longer orbital lifetime.

Testing of supposed Chinese ASAT systems has continued since the destruction of FY-1C in 2007. In 2013, the PRC tested two possible ASAT systems; the first successfully destroyed a ballistic missile with no space debris generation, while the second was allegedly a rocket test. This second test, officially a scientific mission, was tracked on a trajectory towards geosynchronous orbit and reached an altitude of about 10,000km before re-entering the Earth's atmosphere without placing any objects into an orbit (Weeden, 2013: 2). While the launch, which took place on the 13th May 2013, has not been officially acknowledged as a test of ASAT rocket technology, if the allegations are to be believed it indicates that PRC is in the process of developing a ground-based ASAT system capable of reaching Geosynchronous Orbit (GEO) and Geostationary Orbit (GSO).

In addition to the kinetic-kill ASAT system used against FY-1C, there have been reports of the PRC using DEW systems to 'dazzle' French satellites (The Economist, 2010). Dazzling refers to the use of lasers to interfere with the optical sensors of remote sensing satellites. Whilst such interference is often only temporary, lasting as long as an optical sensor is exposed to laser light, sufficiently intense lasers can permanently damage components of an optical system (Wright *et al.*, 2005: 128-129).

4.1.2 Europe and the militarisation of outer space

As discussed above, incorporating outer space within military strategy remains an objective for some spacefaring actors. The prominence of outer space within US military doctrine emphasises the importance of the domain for the US armed forces, and the continued perception of outer space as a battleground (see Joint Chiefs of Staff, 2013b: I-2) arguably implies that future inter-spacefaring actor conflict may involve widespread counterspace operations. Whilst there is no guarantee that any such counterspace operations would affect European space capabilities, it is noteworthy that the North Atlantic Treaty Organisation (NATO), includes "technologies that impede access to space" within "[a] number of significant technology-related trends [… that] appear poised to have major global effects that will impact on NATO military planning and operations" (North Atlantic Treaty Organisation, 2010). Given that NATO operations are largely confined to the geographical region of Europe and that many members of NATO are also members of the EU, it is possible that any counterspace activities directed at NATO Member States may have consequences for the EU.

As described above, there is a substantial history of successful terrestrial ASAT testing, indicating that in the event of a hypothetical conflict between actors with such a capability there would be a credible possibility of ASAT strikes on satellites. In such an eventuality, all satellites orbiting in or near the affected region may well be threatened from space debris generated through the use of ASAT weapons. Consequently, the threat posed by such systems is of serious concern for spacefaring actors, regardless of whether or not they possess ASAT weapons of their own. As will be discussed later in this chapter, the EU is championing the draft Code of Conduct for Outer Space Activities, which includes provisions directed at preventing intentional interference with space objects unless in specific circumstances.

At the time of writing, the highest successful ASAT test is estimated to have taken place at about 1000km (see Dvorkin, 2010: 32; Grego, 2012a: 3; Stares, 1985: 262).[43] Most, if not all ASAT systems have been directed at LEO because of the number of satellites operational there and the expenses associated with developing a missile capable of reaching Middle Earth Orbit (MEO), let alone GEO and GSO (Wright *et al.*, 2005: 135). If the Chinese launch in May 2013 were indeed a rocket test for an ASAT system, it would represent a notable departure from the restriction to LEO. While the rocket was tracked on a ballistic trajectory towards geosynchronous orbit (Weeden, 2013: 2), the altitude reached indicates that such a system could also potentially threaten GNSS and other satellites in MEO. This being said, there are a number of obstacles to developing an ASAT capability directed towards satellites in MEO, including the need to shield the weapons against the high levels of radiation found in the Van Allen Belts (Grego, 2012b).

Assuming that the 2013 Chinese launch was a rocket test, the development of ASAT systems capable of threatening GNSS systems introduces a concern for the EU's critical outer space infrastructures. As discussed in chapter 3, the space segment of the Copernicus programme – which will be divided between LEO and GSO – will not necessarily be critical to the overall programme, which was already partially operational prior to the launch of the first Sentinel satellite. This is not to say however that the loss of a Sentinel satellite directly or indirectly through an ASAT strike would have a negligible impact; not only would it be a loss of an expensive asset which has been many years in

---

[43] Stares (1985: 262) notes that a successful interception was allegedly made by the Soviet Union in 1977 at an altitude of 1575km, however there is conflicting evidence regarding the actual altitude.

development but services relying upon data from that satellite would be starved of input. However, its loss would most likely not be fatal to the wider Copernicus programme, which also uses in-situ data sources. Galileo, on the other hand, will be dependent upon its space segment in order to function. The possibility of space debris being generated in MEO through the intentional destruction of space objects is therefore a disconcerting, even if hypothetical, one.

Non-kinetic interference may also pose a threat to European space programmes in the future, as indicated by allegedly positive results from tests of the US MIRACL system (see Dvorkin, 2010: 36) alongside continued research into DEW technologies (see Webb, 2012) and reports of China dazzling French remote sensing satellites (The Economist, 2010). In terms of the Galileo and Copernicus programmes, such interference is of particular concern for the latter's space segment, which will include remote sensing satellites. This is not say that the Sentinel satellites will necessarily be targeted by entities with DEW interference capabilities, but that the technology to interfere with optical sensors exists and has been employed successfully in the past.

The elements of interdependency and mutual vulnerability are important factors when considering the potential threat posed by ASAT systems to space segments of outer space infrastructures. It must be noted that simply because states have the capability to launch ASAT weapons against targets in MEO or GEO/GSO does not mean that they would necessarily do so in the event of conflict between them and another spacefaring state. As Grego (2012b) points out, China has its own Global Navigation Satellite System (GNSS) satellites in MEO which would be at risk of damage from space debris resulting from an ASAT strike. The same applies to the other two states that have successfully tested ASAT systems. Moreover, if other actors without GNSS satellites of their own were to develop high-altitude ASAT capabilities, it is likely that they would still be dependent upon navigation, positioning and timing signals from a GNSS, making it doubtful as to whether it would be in their interest to generate hazardous debris in a region populated by such critical satellites.

Equally, as O'Hanlon (2004: 24) has discussed with reference to the US ASAT programme, the use of ASAT systems – either in testing or in practice – may lead to a security dilemma for spacefaring states. The warning signs exist already: there was strong military and political support for the resumption of the dedicated US ASAT system following the Chinese test in 2007 (Johnson-Freese, 2009). Additionally, India also expressed an interest in ASAT technology after the destruction of FY-1C, which, as Milowicki and Johnson-Freese (2008) note, increases "the risks of an eventual arms race with Pakistan, Indonesia and other Asian nations" (p. 5). The risk of reciprocation is possibly the most convincing argument against the deployment of weapons in outer space, or even the continued development of ground-based ASAT systems.

4.2 Signal disruption

The use of ASAT systems to disable or destroy orbiting satellites is not the only intentional threat to outer space infrastructures. The Consultative Committee for Space Data Systems (CCSDS) published a Green Book in 2006 which lists a number of common threats to extra-terrestrial operations including, but not limited to: data corruption, attacks against ground infrastructure, the interception of data, jamming, spoofing, unauthorised access, and intentional or unintentional software bugs. Some of these threats may be accidental; for instance errors during coding could lead to bugs in software, whilst data corruption may occur for a multitude of reasons, such as software or hardware failures or interrupted data streams but equally from malicious interference (Consultative Committee for Space Data Systems, 2006a: 3-1-3-2). Unintentional software updates can also lead to problems; in April 2014 the Russian Globalnaya Navigatsionnaya Sputnikovaya Sistema (GLONASS) programme suffered disruption for around 12 hours across the entire GNSS constellation, supposedly because incorrect empherimes data – used to calculate the position of satellites – was uploaded (Cameron, 2014). The disruption meant users of the GLONASS system – as well as users of other systems that use GLONASS to augment the accuracy of their services – received erroneous positional data.

Signal jamming on the other hand is by and large an intentional action; it involves transmission of a radio frequency signal to block or overpower those emanating from a satellite, "[disabling] the means of command and control and data communications, and in this manner render[ing] satellites inoperable or unavailable" (Rendleman, 2010: 6). This technology has been proved effective through its use in a number of scenarios; Iraq is known to have temporarily jammed GPS satellites during operation Iraqi Freedom (Moore, 2005), while Iran has in the past blocked signals from commercial telecommunications satellites (Dant, 2010: 171). However depending on the signals being used by satellites, unintentional jamming is also a possibility. To provide its navigation and positioning services, the GPS constellation, for instance, uses low-frequency signals which have been vulnerable to accidental jamming from Television (TV) stations and Very High Frequency (VHF) transmitters (John A. Volpe National Transportation Centre, 2001: 25-27). Regardless of whether or not the act of jamming is intentional or unintentional, satellite manufacturers and operators have to be aware of the risk that their transmissions may be jammed. As might be expected, some satellite systems are more likely to be targeted than others; in the case of Galileo and Copernicus, the nature of the two systems means that jamming and spoofing – discussed below – are more of a concern for Galileo, which involves a high degree of interaction with users (Anonymous, 2012a; 2013). This prioritisation is reflected in the security measures which are employed; while Galileo’s data transmissions are encrypted, Copernicus’ data is not (Anonymous, 2012a).

Spoofing – or ‘masquerading’, as the CCSDS (2006a; 2006b) calls it – refers to malicious interference whereby persons impersonate a satellite's control centre, issuing commands which may well have a negative or wasteful effect on the mission, or even result in the failure or loss of the satellite in question (Rendleman, 2010: 6). In addition, spoofing can be used to gain access to information or system passwords (Consultative Committee for Space Data Systems, 2006b: 2-5). Although, as Remuss (2009) contends, "[i]t can [...] be assumed that most actors have some capability to detect spoofing, since basic electronic error code checking routines are relatively simple to implement" (p. 35), the inclusion of the issue on the CCSDS list suggests that it remains a concern for satellite operators. Spoofing is a potential problem for both Galileo and Copernicus (Anonymous, 2012a; 2013) however it must repeated once again that for reasons of confidentiality, information pertaining to the protection measures for the Galileo and Sentinel satellites designed to counter jamming and spoofing is not publicly available, other than that telecommands between satellites and ground stations are encrypted (Anonymous, 2012a). Consequently, it is assumed here that the recommendations set out by the CCSDS are similar to those put in place by the EC and ESA. With regards to communications between ground infrastructure and satellites, the CCSDS recommends that systems be designed to cope with breaks in signal transmission, which could occur through loss of line of sight with ground infrastructure or through intentional or accidental jamming (Consultative Committee for Space Data Systems, 2012: 4-3).

The recommendations proposed by the CCSDS concerning jamming and spoofing are not dissimilar to those advocated through Critical Information Infrastructure Protection (CIIP). It appears then that even if outer space infrastructures are not being formally associated with terrestrial critical infrastructure security discourses, the experiences of the latter are informing the practices of the former.

4.3 Congestion as a threat to outer space activities

The weaponisation of outer space and the intentional interference with satellites are not the only threats to the long-term sustainable access to the domain; orbital congestion and frequency allocation are significant existing issues which may only worsen as the exploitation of near-Earth space grows. Although these issues are not necessarily caused through intentional actions, efforts to mitigate them arguably have more in common with the regime-based discourses surrounding sustainable outer space activities than with the preventive approaches directed towards space weather, near-Earth objects and, to some extent, space debris. For this reason, these issues are discussed here rather than in the next chapter.

The increased number of actors launching satellites into the Earth's orbit has led a situation which is often referred to as congestion (Pasco, 2009: 29). This problem is becoming particularly acute in GEO/GSO, where states are assigned orbital slots and radio frequencies by the International Telecommunications Union (ITU) (Moltz, 2008: 311), although crowding is beginning at other orbital altitudes as well. In addition, as Williamson (2012) notes, "[t]he proliferation of micro satellites, many developed by universities or research groups, adds to the potential for crowding" (p. 155). Continued congestion may lead to disruption of critical services and/or collisions between satellites or space debris, generating debris clouds and further increasing the risk of collision. The term 'orbital congestion' is predominantly used in relation to active satellites but space debris also contributes to the problem. If anything, it could be argued that the congestion issue is a consequence of a number of separate issues, ranging from frequency allocation, space debris and a lack of communication and coordination between actors. As Jakhu and Singh (2009) note, “not all radio frequencies and orbital positions are, in practice, useful for all types of users from anywhere. One needs to use only those radio frequencies and orbital positions that are appropriate for one’s use and location of operation” (p. 79). The problem then is one of sustainable practices in the presence of limited resources.

4.5.1 Orbital congestion

In addition to the congestion created by increasing numbers of active satellites, there is also a limitation of the number orbital slots and frequencies available caused by so-called ‘paper satellites’. The ITU distributes slots and radio frequencies to states on a first-come, first-served basis, so some states have been submitting registration applications to the organisation for satellites which may or may not be launched. This has slowed the overall registration process for states with genuine applications and has meant that a significant number of slots and frequencies have been reserved for non-existent satellites (Jakhu and Singh, 2009: 83; Perek, 2004: 223). Despite efforts by the ITU to resolve the problem, Jakhu (2007) argues that they have not been sufficiently effective (p. 184). Although paper satellites may not be a threat to active satellites, they are detrimental to the sustainability of outer space activities as they limit the future usage of near-Earth space and, in particular, GEO/GSO; orbital slots and radio frequencies are finite resources and the inefficient use of them affects most, if not all, spacefaring entities.

The post-mission disposal of satellites in GEO and GSO is another concern for the ITU, and it has been a vocal advocate of so-called ‘graveyard orbits’ above the region (Pasco, 2009: 29). Satellites which are not re-orbited prior to the end of their operational lifetime occupy already limited orbital slots, compounding the growing problem of congestion. The notion of a graveyard orbit involves the delimitation of orbital altitudes into which satellites can be re-orbited to circle the Earth for millennia. This practice is not necessarily without risks however, and there are some ethical concerns associated with the deliberate pollution of orbits above GEO/GSO, particularly if the practice continues over an extended period and efficient debris remediation strategies do not emerge. Graveyard orbits and the potential risks involved are discussed in more detail in the next chapter.

4.5.2 Frequency allocation

All satellites need to communicate at the very least with their respective ground control segments and sometimes, depending on the purpose and mission of the satellite, directly with users. To do this, they require the allocation of radio frequencies free from accidental or intentional interference. Intentional frequency interference has been discussed earlier in this chapter, but the issue of accidental interference is equally significant. The principle behind accidental frequency interference is the same as jamming; the transmission of a signal in the direction of another at a similar frequency will often degrade, block or overpower the second signal (Roberts, 2000: 1102). From the wider perspective of satellite systems as critical infrastructures, guaranteed and secure frequency transmission is necessary not only for the infrastructures themselves to function as expected, but also for their contributions to other terrestrial infrastructures and networks. As an example, as discussed in chapter 3, GNSS satellites play a significant role in what Egan (2007) calls Large Technical Systems (LTSs), enabling the synchronisation of designated critical infrastructures, such as energy, communications and financial systems, across vast geographical expanses. It is conceivable that the disruption of these synchronisation signals would have a debilitating affect upon critical infrastructures dependent upon them.

It is thus imperative for effective and safe outer space activities that frequency allocation be carefully monitored, a task currently undertaken by the Radiocommunication Bureau of the ITU (Henri and Nozdrin, 2012: 187). The issue of regulation in GEO was first discussed at an extraordinary conference of the ITU in 1963 (Collis, 2009; Hitchens, 2007: 176; Vogler, 2000: 112); although both frequencies and orbital slots are reusable, in practice there is a need to prevent congestion. The current legal regime requires individual countries to manage the frequency spectrums allocated to them by the ITU (Robinson, 2010: 38), necessitating a degree of trust that the national agencies or institutions responsible for the frequency management are capable of doing so.[44] Nonetheless, problems remain; not least because "demand far outstrips the available supply of useful frequencies" (Roberts, 2000: 1103; see Collis, 2009), whilst concerns remain over the equitable distribution of frequencies amongst "both developing and developed countries, as well as among civilian and military users" (Robinson, 2010: 39).

4.4 The legal regime on outer space activities

The risks posed by increasing congestion in near-Earth space and technologies capable of interfering with satellite's operations have led to numerous calls for increased international cooperation and coordination towards the creation of a Space Traffic Management (STM) regime (see Ailor, 2006; Cukurtepe and Akgun, 2009; Hitchens, 2007; Johnson, 2004; Lála, 2004; and Sgobba, 2008). Johnson (2004) posits that "[i]n the final analysis, realistic space traffic management has a single aim: to minimize the potential for electromagnetic or physical interference at any time" (p. 80). Although elements of such a regime already exist in the form of the ITU's regulation of orbital slots

---

[44] In the UK, for instance, the Office of Communications (Ofcom) is charged with managing the distribution and regulating the use of the UK's frequency allocation (Ofcom, 2013).

and frequencies (see Hitchens, 2007), few mechanisms are in place regarding the prevention of physical interference, accidental or otherwise. Discussions have taken place at the UN Committee on the Peaceful Uses of Outer Space (UNCOPUOS) regarding how an STM regime or international organisation would complement efforts for long-term sustainability in outer space activities (see United Nations Committee on the Peaceful Uses of Outer Space Scientific and Technical Subcommittee, 2010: 6), but at the time of writing little further progress appears to have been made. However, there are overlaps between an international STM regime and SSA capabilities maintained by some states and being developed by others. For instance, Cukurtepe and Akgun (2009) propose an STM architecture comprising of a 'monitoring and tracking' capability, a 'data management service', an 'operation service' and a 'warning service' (pp. 874-877). Many aspects of this architecture already exist in the form of SSA programmes, albeit structured under national rather than international governance.[45] This is not to say that the system Cukurtepe and Akgun describe would be redundant; an increase in international coordination and data-sharing would most likely have significant positive effects on the safety and security of space-based operations. Nonetheless, should an international organisation dedicated to STM fail to emerge, the foundations for future expansion of data-sharing, or perhaps even data-acquisition, arguably exist in the form of existing national or regional SSA programmes.

Although an STM regime or organisation may not appear likely in the short-term, some legal mechanisms are in place to regulate outer space activities. The legal regime pertaining to outer space activities was first codified in a legally-binding document in 1967 with the signing of the OST. However, the OST was not the first declaration by the UN

---

[45] SSA capabilities, including the European SSA and EU-led Space Surveillance and Tracking (SST) programmes, are discussed in greater detail in Chapter 5 of this thesis.

concerning activities in outer space; the 1963 Declaration of Legal Principles Governing the Activities of States in the Exploration and Use of Outer Space established a series of legal principles, some of which became the foundations for subsequent international law. For instance, Article 2 of the 1963 Declaration includes the provision that outer space and celestial bodies are not subject to national appropriation or imposition of sovereignty, while Articles 7 and 8 establish that jurisdiction over an object is retained by the launching state, which is also liable for any damage caused on the surface of the Earth, in airspace, or in outer space. It is noteworthy that while the 1963 Declaration clearly attaches liability for any damage caused by space objects in outer space to the state of registry (United Nations, 2002: 40), under the 1972 Convention on International Liability for Damage Caused by Space,[46] launching states are only liable for damage caused by space objects in outer space if it is determined that the damage was a result of actions by themselves or persons for whom they are responsible (United Nations, 2002: 14). Consequently, in practice launching states have not been found liable under the 1972 Liability Convention for damage caused by space debris to other space objects. Indeed, the liability convention has only been invoked once, when Kosmos 954 re-entered the Earth's atmosphere over Canada in 1977 (Shaw, 2003: 483) leaving a trail of radioactive debris across parts of the country. There is thus arguably little legal pressure on states party to the Liability Convention to remediate space debris originating from objects for which they are responsible. However, the Liability Convention will be applicable in the event that any de-orbited[47] space objects cause to damage to objects or persons “on the surface of the Earth or to aircraft in flight” (United Nations, 2002: 13).

---

[46] Hereinafter referred to as the Liability Convention.

[47] Space debris remediation, including the practices of de-orbiting and re-orbiting, are discussed in chapter 5 of this thesis.

Activities that may affect celestial bodies or space objects are addressed by Article 9 of the OST:

> [i]f a State Party to the Treaty has reason to believe that an activity or experiment planned by it or its nationals in outer space, including the Moon and other celestial bodies, would cause potentially harmful interference with activities of other States Parties in the peaceful exploration and use of outer space, including the Moon and other celestial bodies, it shall undertake appropriate international consultations before proceeding with any such activity or experiment (United Nations, 2002: 6).

Therefore, according to Article 9, any activity which may result in the generation of space debris should require international consultation before it can go ahead. Theoretically, this would also preclude the use of any equipment or technology which interferes with transmission of signals between satellites and ground segments. However, recent events, such as the destruction of FY-1C and USA-193, suggest that this provision is not being adhered to by spacefaring actors. There can be little doubt that those responsible for the 2007 Chinese ASAT test were well aware of the potential debris generation, particularly given the fact that the Chinese space agency is a member of the Inter-Agency Space Debris Coordination Committee (IADC), and thus they would have been in contravention of Article 9 of the OST. Although the US may have been aware of the Chinese test beforehand (Johnson-Freese, 2009), suspicions do not constitute international consultations. Equally, although the event itself may not have resulted in a comparable debris cloud, it can be concluded from Russian objections that international consultations did not take place prior to the destruction of USA-193 in 2008. Even though the debris cloud from USA-193 was short-lasting, prior to the event there remained a possibility that it could interfere with the operations of other spacefaring actors.

While the OST may prohibit the deployment and use of weapons on celestial bodies, there are no provisions within international law to prevent the weaponisation of outer space. Consequently, other alternatives have been sought to address the issue of space weapons, with the EU currently championing the draft International Code of Conduct for Outer Space Activities.

4.5 European efforts to promote sustainable outer space activities: the draft International Code of Conduct for Outer Space Activities

As discussed earlier, the EU has traditionally approached outer space affairs in a civilian manner reflective of its terrestrial efforts promoting integration. Additionally, since the signing of the ESA Convention in 1975, the agency has had a purely civilian focus, insofar as it will "pursue only the 'peaceful' utilisation of space" (Sheehan, 2007: 88). This reluctance to develop military space capabilities managed by EU institutions meant that that the preparatory stage of Space Situational Awareness Space Surveillance and Tracking (SSA-SST) segment did not include imaging sensors; in this case because ESA members states wished to avoid the SSA having any possible militaristic applications (Anonymous, 2012f). Equally, although the EU has broadened its security agenda in recent years, including in relation to outer space (Pasco, 2009: 6; Sheehan, 2007), it has repeatedly emphasised that the Copernicus project will not have any military applications, despite the inclusion of technologies which have the potential to be considered dual-use. This determination to maintain a civilian space programme means that ESA has not developed any military projects and the EU is directing its efforts towards establishing international agreement over sustainable outer space activities.

In 2006, the United Nations (UN) General Assembly passed resolution 61/75, which in its first paragraph, invites

> all Member States to submit to the Secretary-General before its sixty-second session concrete proposals on international outer space transparency and confidence-building measures in the interest of maintaining international peace and security and promoting international cooperation and the prevention of an arms race in outer space (United Nations General Assembly, 2006: 1)

The call for submissions of ‘concrete proposals’ for Transparency and Confidence-Building Measures (TCBMs) came at a time when there was an impasse at the UN Conference on Disarmament (CD) over outer space affairs. Following the draft resolution entitled ‘Prevention of an Arms Race in Outer Space’ (PAROS), submitted by Italy in 1981, a number of texts had been tabled at the UN attempting to limit or prevent the future weaponisation of outer space, with little success (Rathgeber *et al.*, 2009: 34). Although some progress had been made, the 2006 US National Space Policy compounded existing disagreements by establishing that the US would reject any “new legal regimes or other restrictions that seek to prohibit or limit U.S. access to or use of outer space”, and that “[p]roposed arms control agreements or restrictions must not impair the rights of the United States to conduct research, testing, and operations or other activities in space for U.S. interests” (White House, 2006: 2). TCBMs, on the other hand, are non-binding agreements by actors which have been employed, with some success, in the areas of arms control and nuclear non-proliferation, amongst others. The voluntary basis of TCBMs means that, in theory, actors agree to concessions which they find acceptable, rather than being forced into restrictions which they disagree with. Further concessions then develop as negotiations progress, leading to an incremental regime for the issue in question (Robinson, 2010; 2011c).

The draft International Code of Conduct for Outer Space Activities[48] championed by the EU was first proposed in 2008 under the name the Code of Conduct for Outer Space Activities (Council of the European Union, 2008b; Robinson, 2011). The addition of the word 'international' to the Code's name, although a small alteration, signifies an acknowledgement of the criticism that earlier drafts had been composed without sufficient negotiation with some states. The Code is currently the most likely foundation for a set of TCBMs pertaining to outer space (Robinson, 2010), with the US agreeing to back the initiative, if not the current draft, for the time being (Listner, 2012b). For a variety of reasons, alternatives such as the PPWT – co-authored by China and Russia in 2008 – and PAROS have failed to acquire enough support in the CD and wider UN so far (see Horikawa, 2014: 24; Pasco, 2014: 98). Nonetheless, there is no guarantee that the Code will come to fruition, as a number of obstacles remain. In particular, China, Russia and India maintain their position that a legally-binding treaty is required if any outer space weaponisation regime is to succeed (Listner, 2012b; Pasco, 2014: 98; Robinson, 2012). This is at odds with the 2006 US National Space Policy, as a legally-binding treaty would prohibit the deployment of orbital weapons systems which the US may decide in the future are necessary to its national security. Although the 2010 National Space Policy published by Obama administration takes a much softer tone to outer space affairs, it still maintains the right of the US to defend its space systems and, if necessary "defeat efforts to attack them" (White House, 2010b: 3). There is some ambiguity in this statement, however it could be concluded from the continued presence of space control and space force application within US military doctrine (see Joint Chiefs of Staff, 2013a; 2013b) that the

---

[48] Hereinafter referred to as 'the Code'.

deployment of orbital weapons systems is still regarded as a potential avenue for the future conduct of military operations. On the one hand, the Code needs the support of the US for it to succeed but at the same time the alienation of China, Russia and other actors hoping for a legally-binding treaty may be equally detrimental to the overall objective of restricting any potential weaponisation of outer space.

Despite responsibility over negotiations on the Code having been given to the United Nations Institute for Disarmament Research (UNIDIR) in 2012 (Council of the European Union, 2012: L 140/69), progress appears to have stagnated (Foust, 2012), leaving doubts about the Code’s prospects. Furthermore, although the Obama administration has provided public support to the on-going negotiation processes, in January 2013 President Obama signed the *National Defense Authorization Act for Fiscal Year 2013,* which requires in Section 913 that in the occasion that the US signs any international agreement on outer space activities that is not in itself legally-binding, the President must assure Congress that the agreement “has no legally-binding effect or basis for limiting the activities of the United States in outer space” (United States Congress, 2012: 243). Restrictive though it is, this clause does represent a small concession on behalf of Congress, as the original May 2012 draft Act declares that government funds dedicated to military projects cannot be used to implement any international agreement on outer space activities that has not been ratified by the US Senate (United States House of Representatives, 2012: 205). The result of Section 913 is that not only must Congress be informed of the progress of negotiations on the Code, or any similar international agreement on outer space activities but such agreements must not have legally-binding clauses within them (Listner, 2013), or have the potential to become legally-binding in the future.

It is worth emphasising that despite the reservations of some spacefaring states with respect to the Code, others continue to maintain their support. For instance, the 2014 UK National Space Security Policy states that:

> [i]n **promoting a safe and more secure space environment**, [… the UK] will: [… w]ork with international partners for the earliest and widest possible subscription to norms of responsible behaviour in space, through the proposed international Code of Conduct for Outer Space Activities (HM Government, 2014: 5, original emphasis).

The explicit reference to the Code as a means of promoting norms of "responsible behaviour in space" (HM Government, 2014: 5) is arguably indicating that the UK is declaring support for that initiative ahead of other proposed legal instruments such as the PPWT. This stance is explained by the acknowledgment that "[d]ifficulties in reaching international consensus on aspects of existing space treaties has led to the need for complementary efforts to agree non-legally binding principles for responsible behaviour in space" (HM Government, 2014: 16). Moreover, it is contended that "[i]n pursuing the Code, it is recognised that most activity in space can have dual military and civilian use, but does not seek to define civil or military applications or to prejudge issues before the Conference on Disarmament" (HM Government, 2014: 17). The reference to avoiding definitions of civil or military applications reflects existing debate over the PPWT, which seeks to define and ban space weapons (see Conference on Disarmament, 2008: 3).

Although the future of the Code is by no means assured, the intentions of the EU in drafting and championing it remain relevant. The latest public draft of the Code, made available in June 2012, points to a number of possible dangers to outer space infrastructures, though it is arguably weighted towards the dangers posed by space debris and collisions between space objects.[49] According to the first operative paragraph of the Code, its purpose is to "enhance the security, safety and sustainability of all outer space activities" (European Union, 2013: 2), and it is elsewhere noted that "space debris affects the sustainable use of outer space, constitute [*sic*] a hazard to outer space activities and potentially limit [*sic*] the effective deployment and utilisation of associated outer space capabilities" (European Union, 2013: 2). The inclusion of 'sustainability' within the objectives of the document reflects a wider shift amongst space-faring entities towards the long-term security and safety of human activities in outer space (Arévalo-Yepes *et al.*, 2010; Grego and Wright, 2010; Weeden and Chow, 2012; Williamson, 2012), including an initiative at UNCOPUOS (see Brachet, 2012). The term entered the Code in the 2010 revised draft, replacing "predictability", which appeared in the 2008 version (Council of the European Union, 2008b: 5). This change arguably represents an anticipatory stance on outer space security reflective of precaution and premediation, whereby there is a perceived need to manage future risks and dangers that could emerge from some current activities if left unchecked.

Sustainability in outer space activities is not identical to its terrestrial counterpart; unlike pollution and resource-extraction on Earth little human action can necessarily affect the 'environment' of outer space. Space debris, for instance, while effectively a pollution of the Earth's orbit, does not directly affect the vacuum in which it exists. Perhaps the most significant exception to this is the explosion of nuclear devices in LEO, which has been proven to affect radiation particles in the Van Allen belts surrounding the Earth. The objective of sustainable extra-terrestrial activities is to enable continued safe access and

---

[49] For the purposes of this paper, the paragraphs and articles mentioned or quoted refer, unless stated otherwise, to those in the September 2013 revised draft.

use of outer space through the labelling of certain actions as sustainable/unsustainable or, in other words, positive/negative. As with other mechanisms of anticipatory security, painting activities in a positive or negative light and respectively promoting or condemning them is intrinsically risky as unforeseen consequences, increased knowledge or technological developments may transform the way those actions are perceived.

'Sustainable' outer space activities are often mentioned with reference to space debris (see Brachet, 2012; Williamson, 2012), and indeed much of the section within the Code on safety, security and sustainability is dedicated to the generation of debris in outer space (see European Union, 2013: 5-6). There is already a substantial amount of space debris orbiting the Earth – the US Space Surveillance Network (USSSN) is currently tracking around 23,000 objects with a diameter of 10cm or larger – and it is quite possible that future debris generation could render some orbital altitudes unusable. Kessler and Cour-Palais (1978) predict that should the density of debris at a particular altitude reach a certain point, objects may begin colliding with other objects, leading to a significant increase in debris generation. This chain of events, known as the Kessler Syndrome, has not yet materialised, although the Space Debris Mitigation Guidelines of the Committee on the Peaceful Uses of Outer Space[50] text warns that "fragments generated by collisions are expected to be a significant source of debris" in the future (United Nations Office of Outer Space Affairs, 2010: 1).

Space debris could be considered a 'known' danger as the current debris population is already an issue for current operations in outer space.[51] To an extent, therefore, actions taken to curb its generation or reduce the size of the debris population are not so much

---

[50] Hereinafter referred to as the UN Space Debris Mitigation Guidelines.

[51] To take the International Space Station (ISS) as an example, there were six recorded events between April 2011 and April 2012 where the risk of collision with a piece of space debris was significant enough to require a Collision Avoidance Manoeuvre (CAM). Manoeuvres were successfully conducted in four of these cases, whilst the crew was forced to evacuate to the Soyuz module for the remaining two events as the collision warnings arrived too late (NASA Orbital Debris Program Office, 2012a: 1-2).

anticipating a future problem as trying to stem an existing one. Nonetheless, there is a need to maintain awareness of the possibility of surprise, both in terms of debris generation or the danger posed by existing debris to satellites. As mentioned earlier, alterations to the orbit of a piece of space debris could threaten satellites which were not previously considered at risk of collision. However, it is worth briefly noting that the issue of space debris was largely ignored for the first thirty years of space exploration and exploitation (Crowther, 2003: 157) and the first guidelines aimed at reducing the amount debris generated through good practice only emerged in the 1990s.[52] The notion of sustainable outer space activities aimed at reducing debris generation could be seen as adhering to the precautionary principle; although there is irrefutable evidence that the space debris population is steadily increasing and that collisions between debris and space objects – operational or otherwise – can be destructive, the wider effects of human exploration and exploitation upon the outer space environment are by no means certain. At the time of writing, no orbital altitudes are considered too dangerous for satellite operations, though there is a risk of such a situation arising in the future if current debris generation rates are not reduced. Moreover, just as the issue of space debris did not become apparent for years after the launch of Sputnik in 1957 (Crowther, 2003), it is not inconceivable that other environmental issues may emerge in the future. Signatories to the Code, or any international agreement containing a similar emphasis on sustainability, would thus be committing to a vision of outer space security predicated on the management of future risks in order to ensure continued access to outer space.

In addition, while much of the Code is dedicated to mimising space debris generation through improved TCBMs (Robinson, 2010; 2011) and the avoidance of deliberate collisions and fragmentations in outer space, these measures may have the

---

[52] Space debris is discussed in more detail in chapter 5 of this thesis.

subsequent effect of limiting the likelihood of terrestrial or space-based ASAT systems. As mentioned earlier, the EU's space programme is largely civilian in nature. Only one EU institution – the EDA – openly operates satellites for military purposes, which are mainly communications and remote sensing. Unlike some other spacefaring actors the EU remains, for the time being at least, fervently opposed to the research and development of space weapons. The Code thus represents a diplomatic strategic effort by the EU to secure its critical outer space infrastructures by passively limiting the future use of ASATs. Although the Code is not legally-binding in its current format, should it eventually be signed it would nonetheless represent a commitment by the signatories to adhere to the measures and principles contained within. Of particular importance to ASATs is the paragraph which requests that actors:

> refrain from any action which brings about, directly or indirectly, damage, or destruction, of space objects unless such action is justified […] by imperative safety considerations, in particular if human life or health is at risk; or […] by the Charter of the United Nations, including the inherent right of individual or collective self-defence; or […] in order to reduce the creation of space debris; […] and, where such exceptional action is necessary, that it be undertaken in a manner so as to minimise, to the greatest extent practicable, the creation of space debris (European Union, 2013: 6).

Rather than completely prohibiting the use of ASAT systems, the Code sets out specific situations where the use of such weapons could be justified and, in doing so, arguably seeks to preemptively to constrain future usage. Taking the recent examples of ASAT use, the Chinese test of 2007 against FY-1C and the US destruction of USA-193 in 2008, the latter would be justified under the provisions of the Code as not only was the mission supposedly undertaken to prevent the atmospheric release of toxic fuel upon re-entry of the satellite[53] but the debris cloud created, while substantial, was not long-lasting (Pardini and Anselmo, 2009: 794). The Chinese test, on the other hand, created a debris cloud which, together with the cloud from a collision between two satellites in 2009, constitutes approximately a third of all debris in LEO (NASA Orbital Debris Program Office, 2012b: 2). Although the Code is not legally-binding in its current format, should it eventually be signed it would nonetheless represent a commitment by signatories to adhere to the restricting measures and principles contained within.

Many references to sustainable outer space activities within the Code pertain to space debris generation, although other issues such as orbital congestion, frequency allocation and frequency interference – both accidental and intentional – remain a concern (Williamson, 2012). Along with its provisions pertaining to space debris, the Code calls for signatories to commit to “improve adherence to, and implementation of ITU regulations on allocation of radio spectra and orbital assignments, and on addressing harmful radio-frequency interference” (European Union, 2013: 6). As discussed earlier in this chapter, orbital congestion and frequency allocation are issues which already exist, and can thus be classified as immediate risks to on-going operations in near-Earth space, but they are likely to worsen as the number of objects launched into outer space increases. The requirements of the Code, which include the aforementioned commitment to existing ITU regulations, are directed at increasing inter-actor cooperation through TCBMs, such as notification of

---

[53] There has been some debate about whether the destruction of USA-193 was simply to prevent the dispersion of carcinogenic and toxic chemicals or if it was also a reaction to the 2007 Chinese test and an opportunity to prove that the US maintained a credible ASAT capability. For more on this, see Johnson-Freese (2009: 108-116).

activities undertaken in outer space and the sharing of national outer space policies and information on actors' activities in the extra-terrestrial domain.

The Code can be conceived of as containing mostly precautionary and preemptive principles promoting sustainability in outer space through good practices, international notification of manoeuvres in orbit and avoidance of the deployment or use of anti-satellite weapons systems. On the topic of space debris, the emphasis on minimising rather than preventing debris generation implies an acknowledgement of surprise and unpredictability, even though the generic danger space debris poses to satellites is well known. Notably however, space debris is portrayed in the Code as originating from launcher and satellite operations, with the existing debris population ignored. Whilst the international commitment to space debris mitigation advocated by the Code is important, it is arguably proposed in an unimaginative and restrictive manner; accidental collisions in outer space resulting from the existing debris population are hardly considered and space debris remediation is not mentioned at all. The absence of any considerations for reducing the size of the existing space debris population is indicative of a short-term outlook intended to mitigate the surprise of accidental debris generation by advocating the implementation of UN guidelines. However, by not explicitly committing to develop remediation technologies, the Code arguably fails to anticipate the dangers posed by existing space debris, which represent clearer and more calculable threats to outer space operations than debris generated in the future, of which the size, altitude and direction are obviously unknown. If anything, preemption is arguably being prioritised ahead of prevention.

The issues of frequency allocation and orbital congestion, while existing in the present, are not yet as imminent a danger to the security and safety of outer space infrastructures as space debris. Nonetheless, the preemptive measures contained within the Code are intended to reduce the likelihood that issues caused by a lack of communication, cooperation or coordination between spacefaring entities will appear or worsen, to the stage where they threaten outer space infrastructures. To put it another way, they are oriented towards mitigating the element of surprise which might occur following unannounced manoeuvres or other activities in outer space.

The Code is largely directed at existing or statistically calculable dangers, such as space debris, even if it has long-term precautionary ambitions for ensuring the sustainable access to outer space. These dangers are as much a concern for present outer space activities as they are for future ones, and although there appears to be widespread agreement on the need for increased cooperation and coordination between spacefaring actors, there is still some political reluctance to agree to all of the measures proposed in the Code. The apparent hiatus in negotiations over the Code demonstrates the tension between the ambitions of anticipatory security mechanisms and the politico-bureaucratic reality; the danger posed by space debris to operations in outer space is rooted in historical evidence, as is the potential for substantial debris generation through the accidental or intentional destruction of satellites. However, multinational efforts to prevent the intentional destruction of satellites – exemplified most recently through the Code and the PPWT – have yet to succeed. Analysis of the specific reasons for the failure of each diplomatic initiative exceeds the focus of this thesis, however it could be argued that there is still not enough global political support for the long-term sustainability of outer space activities to overcome existing points of contention. The US is a pertinent example here; the restriction placed upon international agreements containing legally-binding limitations on outer space activities present within the *National Defense Authorization Act for Fiscal Year 2013* is indicative of the continued domestic opposition of practices promoting sustainability in outer space, prioritising instead US national interests (see United States Congress, 2012: 243). Nevertheless, if the Code, or any international agreement containing similar provisions on space debris generation and the intentional destruction of satellites, were to be signed in the future, it would represent a significant commitment to a vision of outer space security foregoing the strategic advantages of ASAT weapons for the sake of future sustainable access to the domain.

4.6 Intentional threats to critical outer space infrastructures and European outer space security

This chapter has explored the forms of intentional interference to which the space segments of outer space infrastructures are vulnerable. It began by introducing the militarisation of outer space, arguing that although it may not be an immediate concern for the security of European outer space critical infrastructures, there is a significant risk that future conflicts may involve widespread counterspace operations given the importance of outer space activities to military strategists. The US, the Russian Federation and the PRC have all successfully tested ASAT weapons systems and have displayed a willingness to continue or resume development of said systems should they feel the need to do so. As an example, in addition to outer space operations being of critical importance to US military doctrine, said doctrine continues to portray near-Earth space as an extension of terrestrial warfare, and includes the concepts of space control and space force application in its doctrinal publications. For this reason, both terrestrial and space-based ASAT systems represent a notable, if only potential, threat to the space segments of European critical outer space infrastructures.

Other forms of intentional interference exist alongside the weaponisation of outer space; particularly signal interference but also satellite and frequency congestion. Congestion may not necessarily be an intentional form of interference but as it largely has man-made origins and the means of mitigation are broadly similar to other man-made risks and dangers, it has been included in this chapter. This being said, space debris has been included in the next chapter as although there have been some instances of intentional debris creation, much of it has been generated through a lack of effective post-mission disposal practices or unintentional fragmentations during launch and operational stages.

The EU has openly acknowledged the need to protect the critical outer space infrastructures upon which European societies depend, and appears determined to do so without resorting to the use of military force. The international legal regime concerning activities does not, for the moment, preclude the deployment of extra-terrestrial weapons and the history of attempts to create a legally-binding ban on such systems – most recently through the PPWT proposed by the Russian Federation and the PRC – does not offer much hope. The EU-championed Code represents a non-legally binding commitment to the sustainable access to and use of outer space through pacifistic means, though many of its provisions concern existing issues such as space debris and orbital congestion rather than weaponisation directly. It is representative of an anticipatory security logic underpinning the EU's approach to mitigating intentional man-made risks to its critical outer space infrastructures, although this logic is for the most part arguably preemptive with elements of prevention. As well as seeking to restrict future debris generation, the Code is arguably attempting to reduce unexpected or unannounced manoeuvres of space objects through TCBMs, thus mitigating the element of surprise to other actors that such manoeuvres can introduce.

Nonetheless, questions persist over the continued dedication to the anticipatory security mechanisms incorporated within the Code. The future of the document is by no means assured, with strong reservations remaining amongst some spacefaring actors. Should no agreement be met soon, it is quite possible that it will become yet another name in the growing list of diplomatic initiatives on outer space affairs that have failed to come to fruition.

The following chapter turns to environmental risks and dangers which may threaten outer space infrastructures. As mentioned above, space debris is one of the most significant of these risks and dangers alongside space weather phenomena. Just as the Code is representative of a logic of anticipatory security in the diplomatic sphere, the EU is beginning to develop an independent SSA capability to forewarn operators of impending collisions and space weather events.

5 Environmental hazards to the security of critical outer space infrastructures

Chapters 2 and 3 argued that outer space assets are critical both to a number of societal functions and to a host of European Union (EU) policies. Interference in the functioning of these assets may well have detrimental effects upon terrestrial societies and EU-policy making. The forms of intentional interference discussed in the previous chapter are by no means the only security risks which need to be considered by actors involved in outer space affairs. Environmental phenomena have the potential to damage or destroy man-made assets in outer space: radiation and space weather phenomena can damage and disrupt the electronics on board spacecraft whilst space debris, one of the most important extra-terrestrial risks to satellites (Hitchens, 2007; Moltz, 2008; Wright, 2007; 2009; Vogler, 2000), is an ever-increasing danger.

In a similar fashion to the draft International Code of Conduct for Outer Space Activities discussed in the previous chapter, the measures undertaken by the EU and its affiliated agencies to counter and mitigate the effects of extra-terrestrial environmental hazards are analysed in the framework of anticipatory security. As discussed previously, anticipatory security commonly takes the form of preventive or preemptive action and this chapter makes the case that with regards to environmental security in outer space, the EU has taken a largely preventive approach. Many risks that are being countered or mitigated are already proving dangerous to on-going operations and thus although there is an element of sustainability at play, the measures discussed in this chapter are designed to secure the present as much as the future. There is also some discussion of whether existing responses to environmental risks in outer space conform to terrestrial critical infrastructure resilience or protection strategies.

5.1 Natural environmental risks

To begin with, it should be noted that for the purposes of this thesis, natural environmental risks are considered as those present within the vacuum of outer space and the gravitational well of the Earth which may affect Earth-orbiting satellites. Consequently, the possibilities of microbial life on the Moon or other celestial bodies, or any chance of human exploration contaminating those celestial bodies, are not being debated here. This should not be taken as a devaluation of man-made debris being left on celestial bodies; that issue, as highlighted by the decision in December 2012 to crash two satellites into the Moon (Amos, 2012c), is of great importance and deserves an in-depth analysis of current procedures[54] but it lies outside of the focus of this thesis.

5.1.1 Radiation and space weather

It should be noted from the outset that radiation and space weather are complex phenomena and it is beyond the context of this thesis to account for them in great detail. Consequently, what follows is a relatively basic introduction to radiation and space weather and the impacts they can have on satellites and, subsequently, satellite operators and terrestrial societies.

One of the primary concerns for actors involved in extra-terrestrial exploration and exploitation is radiation. The Earth is surrounded by the inner and outer Van Allen radiation belts, where energetic charged particles – electrons and protons emanating mainly

---

[54] For instance, the decision to crash the satellites was taken to avoid possible damage to lunar landing sites identified as being heritage sites of human exploration (Amos 2012c), which raises questions about the prioritisation of human structures and debris on the Moon over the natural landscape.

from the sun – are trapped by the Earth's magnetic field (Ganushkina *et al*., 2011). These particles have numerous effects, among which is an increased degradation of power produced by solar panels to the effect of around 5% annually, compared to a predicted degradation rate of around 2% for satellites orbiting outside of the Van Allen belts (Odenwald *et al.,* 2006: 283). The Van Allen belts were first discovered by a sensor, designed by American physicist James Van Allen, carried on board Explorer I in 1958 (Krige and Russo, 2000: 20). The inner belt begins at around 200-1,200km depending on latitude, and extends to around 10,000km in altitude. In this belt, the strongest radiation can be found at 3,500km. The outer radiation belt, meanwhile, begins at about 10,000km in altitude and extends to 84,000km, with the highest concentration found around 16,000km. However, when exposed to sunlight, the size of the outer belt is reduced, extending to about 59,500km (Dolman, 1999: 99). There is also an area located roughly above the South Atlantic called the South Atlantic Anomaly, where, because the Earth's magnetic field is tilted with respect to the Earth's axis, the end of the lower Van Allen belt is lower than the rest of the belt. Satellites on polar sunsynchronous orbits regularly fly through this region and will experience higher exposure to charged particle radiation (Anonymous, 2010e). The potential disabling effects of the radiation present in the South Atlantic Anomaly were illustrated in 2010, when the United States Air Force (USAAF) launched the first satellite of the planned Space Based Surveillance System (SBSS) only for it to suffer electronic problems after flying through the region. These problems accorded significant delays and only in August 2012 was it announced that the satellite was eventually ready to begin operations (Reuters, 2012).

In addition to the Van Allen belts, Space Weather Events (SWEs) emit substantial amounts of radiation, interfering with communications between satellites and their ground stations (Allianz Global Corporate & Speciality, 2012: 12; House of Commons Defence

Committee, 2012). Consequently, satellite manufacturers and operators have to carefully consider the planned operations for each satellite, as the protection requirements will differ depending on the intended altitude and orbit (see Allianz Global Corporate & Speciality, 2012: 12; Baines, 2004).

Radiation from SWEs threatens both satellites and terrestrial infrastructures (House of Commons Defence Committee, 2012), with many of them originating from solar geomagnetic storms (Allianz Global Corporate & Speciality, 2012: 12). For the purposes of this thesis, the definition of space weather adopted by the United States National Space Weather Program (2011) – "conditions on the Sun and in the space environment that can influence the performance and reliability of space-borne and ground-based technological systems, and can endanger human life or health" – will be used. There are three basic types of SWE: Coronal Mass Ejections (CMEs), charged energetic particle bursts – otherwise known as Solar Energetic Particle (SEP) events – and solar flares, although the House of Commons Defence Committee (2012) includes solar radio bursts in their list (p. 10), despite them being a consequence of the other SWEs.

The most 'basic' type of SWE is the solar flare, which is an emission of electromagnetic energy from the Sun. CMEs involve the ejection of plasma from the Sun's atmosphere, usually violently and into interplanetary and interstellar space, while SEPs are ejections of charged energetic particles. All these SWEs can take place on their own or in combination with each other, with solar flares commonly but not always, taking place alongside CMEs and SEPs, and they all emit radiation, either in electromagnetic or energetic particle form. In addition to the charged protons and electrons emanating from the Sun through CMEs and SEPs, ionised heavy elements are also released (Anonymous, 2012e). The largest recorded SWE took place in September 1859 and is now known as the Carrington Event. The SWE began with a "solar flare so strong that it could be seen with the naked eye" (House of Commons Defence Committee, 2012: 10). The solar flare was followed by a huge CME which disrupted telegraph systems on Earth, to the extent that "[o]perators were able to disconnect their batteries and continue to send messages using only this induced current" (Committee on the Societal and Economic Impacts of Severe Space Weather Events: A Workshop,[55] 2008: 7; see also House of Commons Defence Committee, 2012: 10).

When it comes to radiation, there are, as mentioned above, two types associated with SWEs: electromagnetic and energetic particle radiation. While energetic particle radiation consists, as described above, of highly charged protons and electrons, electromagnetic radiation involves a flash of light visible at all wavelengths, including Ultra-Violet (UV) and x-ray (Anonymous, 2012e). There are also sometimes emissions of solar radio bursts at radio frequencies which can impact technologies relying upon those frequencies (House of Commons Defence Select Committee, 2012).

Although satellites "appear to be remarkably robust against most space weather events encountered during the last 30 years" (Odenwald *et al*., 2006: 280), the potential danger posed by radiation emanating from extreme space weather should not be ignored; extreme space weather is commonly described as low-frequency/high-consequence (LF/HC) by studies of its impact on outer space infrastructures (see CSEISSWE, 2008: 6). In 2010, an Intelsat-owned geostationary satellite named Galaxy 15 suffered a communications failure after allegedly being exposed to high-levels of electromagnetic radiation from a solar flare (Allianz Global Corporate & Speciality, 2012: 12). Although communications between the ground control and Galaxy 15 were eventually resumed and the satellite recovered, the example nonetheless highlights the dangers posed by extreme SWEs.

---

[55] Hereinafter referred to as the CSEISSWE.

Charged energetic particle radiation can also cause significant damage to satellites as they can sometimes penetrate through the aluminium skin of the satellite and reach the fragile electronic components. If this happens, the radiation can cause transient failures known as Single Event Upsets (SEUs), whereby there is a change of state in the electronics which can interfere with any programmes being run at the time, necessitating a reboot of the satellite. Additionally, a satellite's photoelectric components can be damaged; with solar cells suffering wearing from the bombardment of charged protons and electrons, whilst imaging equipment can be distorted if the radiation is particularly dense. Finally, charged energetic particle radiation can also disrupt sensors which control a satellite's attitude, in which case the attitude has to be controlled manually (Anonymous, 2012e).

In addition to the immediate effects of radiation upon satellites and their components, long-term damage can also be caused. A 2013 report by the Royal Academy of Engineering, assessing the potential dangers posed by an extreme SWE, notes that:

> the significant cumulative radiation doses would be expected to cause rapid ageing of many satellites. Very old satellites might be expected to fail in the immediate aftermath of the storm while new satellites would be expected to survive the event but with higher risk thereafter from further (more common) storm events (Royal Academy of Engineering, 2013: 5).

It is thus important for satellite owners and operators to bear in mind the erosion of long-term operational capacity caused by space weather as well as the short-term damage that may result from SWEs.

As well as the physical effects of SWEs on satellites, a further consideration is the economic impact of losing satellites' operational capabilities through SWEs. Odenwald *et* *al*. (2006) attempt to model the financial implications of such an eventuality, although they note that such estimations are difficult as there is no standard formula for publishing the costs of a satellite, so there is little means of knowing whether the published prices include launch costs as well as hardware, or even insurance (p. 282), and many satellite operators do not reveal the economic successes or failures of their operations (p. 283). Odenwald *et al*. model an extreme SWE three times as severe as the 1859 Carrington Event, concluding that such a ‘superstorm’ would lead to “potentially major economic and military impact on our space assets”, and that “[u]nlike previous historical events, our current reliance on satellite technology and human activities in space, [*sic*] place us in a unique and unprecedented nexus of vulnerabilities from such an event” (p. 294). Additionally, the GPS constellation – and presumably by association the Galileo, Globalnaya Navigatsionnaya Sputnikovaya Sistema (GLONASS) and Beidou constellations – would most likely be affected, with significant errors in the positioning data being transmitted and possible temporary or permanent failures of satellites, necessitating replacements, leading to GPS ‘blackouts’ at periods when too few satellites are visible to receivers (p. 294-295). Although these scenarios are of course based on scientific and mathematical models of a “worst-case” (p. 282) ‘superstorm’, they are nonetheless indicative of the vulnerabilities of terrestrial societies to extreme SWEs.

5.1.1.1 Forecasting and monitoring SWEs

There are currently two forms of defence against radiation damage to satellites: mitigating damage through forecasting SWEs and protection through design. The forecasting of SWEs is undertaken by the agencies, mainly of individual states, charged with the monitoring of space weather. However, there is a long-running history of cooperation and collaboration between those agencies, as space weather is considered phenomena necessitating a global forecasting effort. Most of the data on space weather gathered by ground-based and *in situ* sensors is shared between agencies, with the exception of data gathered by some military satellites, which could reveal the orbits of said satellites (Anonymous, 2012e).

The majority of US efforts to forecast and monitor SWEs are undertaken by the National Oceanic and Atmospheric Administration (NOAA) – specifically the Space Weather Prediction Centre (SWPC) – and the USAAF’s Weather Agency (AFWA). These two agencies are responsible for SWE data requirements of the civilian and military spheres respectively, whilst the National Aeronautics and Space Administration (NASA) is also involved from a scientific, rather than operational, perspective. US SWE forecasting relies upon data from a number of ground-based and *in situ* sources, including, but not limited to, NASA’s Advanced Composition Explorer (ACE) and the NOAA’s Geostationary Operational Environmental Satellite (GOES) and Polar Operational Environmental Satellite (POES).

Within Europe, space weather studies take place at both the European and national levels, with the European Space Agency (ESA) conducting the forecasting and monitoring of SWEs at the European level through the Space Situational Awareness SWE segment (SSA-SWE). Although the SSA has only recently completed its preparatory stage, the space weather segment has benefited from existing European expertise and ground-based and *in situ* sensors, to the extent that ESA has “been able to establish a federated precursor service system, that is utilising existing national space weather assets and services” (Anonymous, 2012e). With regards to dedicated satellite missions, ESA relies, like the US forecasting efforts, on the ACE and the Solar and Heliospheric Observatory (SOHO) missions, which are both based at the first Lagrange Point, otherwise known as L1. The advantage of using L1 for SWE forecasting and monitoring is that it is at an Earth-Sun gravitational equilibrium around 1,500,000km from the Earth and 148,500,000km from the Sun, allowing for relatively stable orbits (Anonymous, 2012c; Christian and Davis, 2012). Additionally, the distance from the Earth means that the solar view of satellites based there will not be periodically eclipsed by the Earth as it travels through outer space (National Aeronautics and Space Administration, 2012). Consequently, to take the ACE mission as an example, it “has a prime view of the solar wind, interplanetary magnetic field and higher energy particles accelerated by the Sun, as well as particles accelerated in the heliosphere and galactic regions beyond” (Christian and Davis, 2012). However, despite the advantages of using L1 for solar monitoring, satellites located there can only provide “15 to 30 minutes’ warning in regards to CME-related effects which dominate many of the most important impacts of a superstorm” (Royal Academy of Engineering, 2013: 14). Consequently, plans have been proposed to send satellites closer to the Sun to allow the opportunity for earlier warnings of geoeffective SWEs. NASA’s Sunjammer mission, due to launch in 2015, will act as a demonstration mission for solar sail technologies enabling closer studies of the Sun. It will also carry a solar wind analyser and magnetometer in order to begin providing improved forecasting and monitoring of solar winds (National Aeronautics and Space Administration, 2013; Royal Academy of Engineering, 2013: 14).

Data on space weather and the outer space environment is also acquired by sensors placed on non-dedicated spacecraft, such as geostationary meteorological satellites and the Galileo satellites (Anonymous, 2012e). Although these sensors can, depending on their purpose, provide data on the environmental surroundings of their host satellites or of solar activity, they are limited by the fact they are placed on satellites designed to face the Earth and therefore may not have sight of phenomena SWE forecasters are particularly interested in. Nonetheless, it is notable that the outer space segments of satellite networks, such as

Galileo, are being employed as part of the system of forecasting and monitoring of the SWEs which threaten them.

The SWE segment of the European SSA contains both preventive and preemptive elements. On the one hand, it involves the forecasting of imminent extra-terrestrial phenomena in order to warn satellite operators of fluctuations in the solar and near-Earth environments, making it a reactive security mechanism enabling calculable probabilities based upon pre-existing solar activity. However, there is a preemptive aspect to its operations insofar as the solar activity which produces space weather events cannot be predicted. Moreover, the segment includes research undertaken into significant SWEs for which there is little historical data.. A number of studies have considered the effects that a severe SWE on a similar scale to, or larger than, the Carrington Event might have on terrestrial and extra-terrestrial infrastructures (see CSEISSWE, 2008; Odenwald *et al*., 2006). In addition, and although not strictly part of the SSA-SWE segment, the sensors which have been placed on board the Galileo satellites (Anonymous, 2012e) are providing data concerning radiation levels in Middle Earth Orbit (MEO). As well as contributing to the development of more robust satellites, this research is also serving to condition those working with vulnerable infrastructures to the possibility and danger of a severe SWE, improving their preparedness if faced with a phenomenon of similar magnitude to the Carrington Event. These studies and practices are contributing to the development and refinement of imaginaries concerned with the impact of future significant space weather events. Nothing can be done to prevent or stop an SWE but increased levels of awareness and preparedness amongst those who deal with the consequences may lead to more effective damage limitation and recovery, enhancing the resilience of affected infrastructures.

5.1.1.2 Protection through design

The common method of satellite protection against radiation – both natural and man-made – is through hardening, which involves designing and testing electronic components so that they are resistant to both electromagnetic and energetic particle radiation.

With regards to the US, satellites used for military purposes are commonly hardened more than civilian ones, a state of affairs which Baines (2004) posits could be "because private sector operators do not recognize the need for their systems to survive nuclear war or other nuclear weapon detonation events" (p. 163). However, a more mundane reason for the lack of commercial hardening could well be financial; hardened components are expensive and consequently commercial and scientific operators have turned to cheaper alternatives, such as shielding and radiation-tolerant parts (Lum *et al.* 1997: 2026). Although the possibility of a nuclear war or explosion may be minimal, it is nonetheless telling that the main concern of much of the astropolitical literature is geared towards warfare, rather than the natural radiation present in near-Earth space. This military focus is, as discussed in chapter 4, representative of a wider obsession with weaponisation and military security present within astropolitical literature, although there is some justification for the fears over exo-atmospheric nuclear detonations.

Another method of protecting satellites and their operational capabilities is through the use of software capable of error-detection. Such software would compensate for SEUs caused by radiation penetrating the aluminium skin of the satellite and potentially reduce the need for extensive radiation hardening of the electronics. However, for such error-detection software to function correctly there must be no physical damage to a satellite's electronics (Odenwald *et al.*, 2006: 292). Although, as Koons *et al.* (1999) note, reported physical damage caused by radiation is a "surprisingly infrequent" occurrence, which they believe may be due in part to "conservative" approaches to component hardening by satellite manufacturers (p. 7), it is nonetheless a possibility necessitating the continued hardening of electronic components.

An important design feature of satellites and their surrounding infrastructure is their resilience. There are a number of ways to increase the resilience of an outer space infrastructure, depending upon the nature of a satellite's mission, the service it offers and its wider infrastructural architecture. These means are not necessarily specific to particular risks or dangers and therefore they will be discussed later in this chapter.

5.1.1.3 Manipulation of the near-Earth outer space environment

Because the Van Allen belts are made up of charged energetic particles, they are extremely sensitive to man-made events, namely atmospheric and exo-atmospheric nuclear explosions. This danger was illustrated when, in July 1962, the US detonated a 1.4 megaton hydrogen bomb at an altitude of 248 miles. The bomb, named Starfish Prime, was part of Project Fishbowl, the US atmospheric and exo-atmospheric nuclear testing programme. The explosion led to a significant increase in the number of electrons present in the Van Allen belts (Moltz, 2008) and the Electromagnetic Pulse (EMP) discharge eventually disabled six satellites: one British, one Soviet and four American (Hoerlin, 1976: 25-26).

Whilst the risk of radiation from nuclear weapons testing or warfare has been secured against by the US military – to the extent that some of its satellites designed for military purposes are hardened against radiation – as mentioned above, Baines (2004) notes that the same is not true for US civilian satellite missions. This may not be due to an ignorance of the threat of nuclear warfare in outer space but rather a consequence of the inevitable balancing act which occurs when weighing up security and finances. Although nearly every aspect of security, at whichever level chosen for analysis, involves some form of consideration for financial viability, this is even more relevant for the physical protection of satellites. Because of the high costs of launching satellites, any additional weight or expensive production techniques must be thoroughly justified.

In the case of radiation, it would appear that the possibility of a nuclear explosion in outer space is not thought probable enough to merit counter-measures. Indeed, the 2006 Consultative Committee for Space Data Systems (CCSDS) Green Book *Security Threats Against Space Missions* does not list nuclear radiation as either a passive or active threat to satellites (Consultative Committee for Space Data Systems, 2006a). The only mention of radiation in the publication pertains to radiation originating from communications hardware. It should be noted that the security threats under consideration in the 2006 Green Book are largely human-focused, in that they are generally instigated intentionally or unintentionally by humans. Nonetheless the absence of warning against radiation emanating from an exo-atmospheric nuclear explosion is telling. As for natural radiation, such as that present in the Van Allen belts, there is no mention of it either in the CCSDS 2006 Green Book, even though space debris is mentioned on two occasions as threats present in the outer space environment which are not present in other terrestrial environments.

5.1.2 Near-Earth Objects (NEOs)

It is worth briefly mentioning NEOs, as research in this field is steadily growing; these are natural hazards such as asteroids with the potential to cause significant terrestrial damage. The risk of NEOs hitting the Earth is arguably one of the more widely-known extra-terrestrial environmental factors, with visible geological evidence of historical events and numerous films using the scenario as a foundation.[56] It has been estimated that around 100 tonnes of meteoroidal mass impacts the Earth's atmosphere every day (Gattolin, 2013: 5) but meteorites – that is to say meteoroids which survive impact with the Earth's atmosphere – large enough to cause terrestrial damage are relatively rare. Moreover, the NASA Near Earth Object Program only classifies asteroids as "potentially hazardous" if they have a diameter larger than 150m and have an orbit which falls within specific restrictions (NASA Near Earth Object Program, 2013). Nonetheless, the potential threat posed by NEOs to terrestrial societies has been acknowledged by states, with the UK in particular lobbying for increased international and regional coordination on the matter, including a focus on NEOs in the European SSA. Additionally, an international committee on NEOs, similar to the Inter-Agency Space Debris Coordination Committee (IADC), has been mooted in an attempt to foster international cooperation on efforts to mitigate or counter the risks of an NEO collision with the Earth (Anonymous, 2012d).

Although NEOs with a diameter larger than 10m present a danger to terrestrial societies, the risk of collision with satellites orbiting the Earth is, in the words of an employee of the UK Space Agency (UKSA), "negligible" (Anonymous, 2012d). Recent research indicates that small meteoroidal particles may have been responsible for damage to satellites – including the failure of ESA's Olympus satellite in 1993 and loss of stability of the Landsat-5 satellite in 2009 (Close *et al.*, 2011: 1-2) – through the generation of electromagnetic pulses upon impact with space objects (Close *et al.*, 2011; Firth, 2013). However given the size of the particles in question, it remains difficult at the time of writing to ascertain with any certainty the danger posed by meteoroids. Consequently,

---

[56] In recent decades, *Armageddon*, directed by Michael Bay, and *Deep Impact*, directed by Mimi Leder, are examples of high-grossing films which depict an NEO on course to collide with the Earth. Although the success of terrestrial efforts to counter the threat varies, the potential widespread destruction resulting from an NEO collision is clearly emphasised in both films. Another film of note is *Meteor*, directed by Ronald Neame and released in 1979, which combines the threat of an NEO about to collide with the Earth with the political tensions of the Cold War.

although aspects of the SSA dealing with NEOs are discussed below, the risk of NEOs colliding with spacecraft is not considered significant enough to be a credible threat necessitating further detailed discussion. The subject has been briefly included within this thesis as the NEO segment is a significant element of the European SSA, yet the author felt it important to emphasise the low risk posed to the space segments of European critical outer space infrastructures.

Both existing and planned efforts to identify NEOs on a potential collision course with the Earth revolve around an increased knowledge of NEOs and their orbits. Much of these efforts involve the deployment of terrestrial sensors to identify and track NEOs. Alongside space weather and space debris, NEOs are an important aspect of the European SSA and to this end, the SSA NEO Coordination Centre opened in May 2013 at ESA's European Space Research Institute (ESRIN) in Italy. The NEO Coordination Centre provides the precursor services that were established during the preparatory stage of the NEO segment of the SSA (SSA-NEO) (European Space Agency, 2013d).

Of all the segments of the SSA, the area devoted to NEOs is the most preemptive in nature. The risk of an NEO colliding with the Earth is relatively small, yet there is substantial financial and political backing for the detection of these astronomical phenomena. To this end, the SSA-NEO segment is charged with searching for asteroids with a trajectory which may lead to them impacting the Earth, as well as contributing to the research and development of methods to deflect NEOs (European Space Agency, 2013d). The development of deflection technologies is particularly preemptive, as it deals with a threat that will remain unclear until an NEO is identified as being on a collision course with the Earth. Nonetheless, once an NEO is identified as having a trajectory that may lead it to collide with the Earth, the SSA-NEO segment will become preventive as it seeks to calculate the probabilities of such a collision, as well as develop technologies to mitigate the threat.

5.2 Space debris

Natural phenomena are not the only environmental risks to orbiting satellites. Although early satellite development and design planned for natural debris (meteoroids) as the main environmental risk to missions, this changed after nearly 30 years of space exploration and exploitation with the recognition of the increasing man-made space debris population in near-Earth space (Crowther, 2003: 157). The first comprehensive report on space debris, published by the American Institute of Aeronautics and Astronautics in 1981 (International Academy of Aeronautics, 2005: 9), warns that the issue would become an "unacceptable risk" (American Institute of Aeronautics and Astronautics, 1981, cited in Deudney, 1985: 283) to orbital operations by the 1990s. Indeed, by 1995, NASA was warning that there was a "significant debris environment" present in LEO (National Aeronautics and Space Administration, 1995: 13). The need for states to consider space debris in the planning of their space programmes and projects has now become widely accepted (Hitchens, 2007: 173) and the threat posed by the problem has even made proponents of anti-satellite (ASAT) weapons consider their positions (see Bormann, 2012: 84). Although there is substantial debate over the definition of space debris (see Listner, 2012c), this thesis will use the definition offered by the United Nations (UN) Space Debris Mitigation Guidelines, which describes space debris as "all man-made objects, including the fragments and elements thereof, in Earth orbit or re-entering the atmosphere, that are non-functional" (United Nations Office for Outer Space Affairs, 2010: 1). Given this definition, as soon as a satellite loses battery power or suffers a communications or power malfunction, it becomes considered as debris and, unsurprisingly, this means there is a significant amount of man-made debris orbiting the Earth. Additionally, spent rocket stages used to propel payloads into their intended orbit become debris the moment they end their planned function. Although there might be a legal argument to separate between debris that is generated as part of a mission's operations and cessation of said operations, debris that is accidentally generated through on-orbit break-ups and debris which is intentionally generated through deliberate collisions or explosions, such differentiation would be of little practical use post-generation. Certainly, in terms of liability and mitigation, the intentional generation of debris, or accidental generation through malpractice, should be identified and criticised. However, with regards to the remediation of debris, which will be discussed in more detail later, the origins of the debris being remediated makes little practical difference, although it may affect the legal conditions under which remediation is made possible.

Most of the debris in Lower Earth Orbit (LEO) will burn up in the Earth's atmosphere within 25 years of its generation, however debris with perigee altitudes higher than 700km may remain in orbit for hundreds of years (National Aeronautics and Space Administration, 2009: 22). Given its possible long-lasting existence, space debris is an ever-growing problem for currently operational and future satellite missions, to the extent that Babintsev (2010) warns "there will soon be a pollution challenge in near-Earth space to add to the already acute problem of environmental pollution on Earth" (p. 22).

Further complication is caused by the fact that the issue of space debris is not static and nor does its growth progress at a linear rate. In 1978, Kessler and Cour-Palais predicted that

> [b]ecause many of these satellites are in orbits which cross one another, there is a finite probability of collisions between them. Satellite collisions will

> produce a number of fragments, some of which may be capable of fragmenting another satellite upon collision, creating even more fragments. The result would be an exponential increase in the number of objects with time, creating a belt of debris around the earth (Kessler and Cour-Palais, 1978: 2637).

In other words, the more debris that there is orbiting the Earth, the higher the risk of collisions between pieces of debris or between debris and operational satellites. To come to this conclusion, which has become known as the Kessler Syndrome, Kessler and Cour-Palais (1978) apply the concept of "mutual collisions", which they argue, "is thought to have been responsible for creating most of the asteroids from planetlike [*sic*] bodies", to a formula for predicting the growth of a debris belt around the Earth (1978: 2637). However, it is worth noting that while

> [t]he time scale in which this [mutual collisions] process is taking place in the asteroid belt is of the order of billions of years. A much shorter time scale in earth orbit is suggested by the much smaller volume of space occupied by earth-orbiting satellites compared to the volume of space occupied by the asteroids (Kessler and Cour-Palais, 1978: 2637).

Space debris is currently generated in one of two fashions: "(*a*) accidental and intentional break-ups which produce long-lived debris and (*b*) debris released intentionally during the operations of launch vehicle orbital stages and spacecraft" (United Nations Office of Outer Space Affairs, 2010: 1, original emphasis). The second means of generation was of particular concern from the 1970s onwards, as it came to light that defunct spacecraft and launcher stages were a significant part of the growth of debris in geosynchronous orbit (GEO) (Anselmo and Pardini, 2008: 1091). However, the United Nations Office for Outer Space Affairs (UNOOSA) warns that this situation of dual-generation may develop in the future towards the scenario predicted by Kessler and Cour-Palais (1978), as “fragments generated by collisions are expected to be a significant source of debris” (United Nations Office of Outer Space Affairs, 2010: 1).

Unintentional collisions between man-made objects have already taken place in near-Earth space: the first confirmed collision took place in late 1991 between the Russian navigation satellite Cosmos-1934 and debris from Cosmos-926, although it was not confirmed until years later (NASA Orbital Debris Program Office, 2005). The first collision identified at the time occurred on the 24th July 1996 between a French military reconnaissance satellite named Cerise and a fragment from an Ariane-1 H-10 upper stage which had exploded ten years earlier (Klinkrad, 2007: 955). Then, on February 10th 2009, the satellite Iridium-33 collided with Cosmos-2251 at an altitude of 790km (491 miles) (NASA Orbital Debris Program Office, 2009). It was the first time two intact satellites had collided in orbit and the energy involved in the impact was over a thousand times higher than that involved in the Chinese ASAT test of 2007 (Marks, 2009). The collision served as a reminder that “even though the heavens are vast, the orbital planes above the Earth are finite, and there are few, if any, rules of the road when the traffic within that finite space becomes congested” (Listner, 2012c). Although the collision occurred within LEO, it will most likely take decades for debris from the event to re-enter the Earth’s atmosphere. In July 2012, NASA noted that 90% of the debris from the Iridium-Cosmos collision and FY-1C destruction was still in orbit, with the debris clouds emanating from the Cosmos-2251 and FY-1C satellites encircling the Earth and the debris from Iridium-33 still largely continuing on polar orbits, like its parent satellite (NASA Orbital Debris Program Office, 2012b). Furthermore, in late September 2012, NASA confirmed that the International Space Station (ISS) may have to be moved in order to avoid a piece of debris from Cosmos-2251 (Stoker, 2012).

Collisions between satellites and debris are not limited solely to LEO and MEO. Ailor (2004) predicts that there is around a one in ten chance of a collision involving a satellite in GEO/GSO in the next decade. Although the timespan for that prediction is running out, that the risk of collision exists at that altitude cannot be over-emphasised. Many of the satellites in GEO/GSO are providing communication services which are integral to both civilian and military walks of life.

The risks posed to satellites by space debris are considerable: because of the distances involved, only objects larger than 10cm in diameter in LEO and larger than 1m in GEO/GSO can be reliably detected and tracked (Anonymous, 2012f; Crowther, 2002: 1241). Numerous terrestrial institutions are involved in the detection and tracking of objects orbiting the Earth, including the US Space Surveillance Network (USSSN), which has the largest network of sensors and consequently maintains the most comprehensive catalogue of space objects. The USSSN currently tracks 22,000-23,000 objects in the Earth’s orbit. Of these, information on 16,000 is publically available, with data pertaining to the remaining 6000-7000 restricted either because of the classified nature of the objects, or because the data is not accurate enough (European Commission, 2013a). With regards to the dissemination of information on space debris, bilateral agreements have been formed between the US and other spacefaring actors (Anonymous, 2012f). However, as noted above, only objects 10cm or larger are tracked by the USSSN and other catalogues. Of the smaller debris, it is estimated that there is around 700,000 pieces of debris 1cm in size, and 130,000,000 pieces of debris at around 1mm in size (Anonymous, 2012c). Debris between 1-10cm is what Crowther (2002) calls the ‘lethal population’:

> because they cannot be tracked or catalogued, yet they can catastrophic damage when they collide with another satellite. Objects smaller than 1 cm may disable a satellite on impact but can be defeated by physical shields; they are termed the risk population (p. 1241).

Because of the astrophysical nature of orbits, the velocities involved in any collision between satellites are extreme (Babintsev, 2010), hence the destruction that can be caused by a relatively small debris fragment.

To take a brief digression into terminology, it is worth noting that whilst the UN and the IADC use the term space debris, the US and, unsurprisingly therefore, NASA prefer the name orbital debris. Although NASA's justification for using the term orbital debris to refer to man-made objects is that space debris includes meteoroidal as well as man-made debris, the difference is largely cosmetic as all parties refer to the same risks and possible solutions. Nonetheless, it is worthwhile briefly explaining the preference in this thesis for 'space' over 'orbital'. The main drawback with the term orbital, and indeed probably the most obvious one, is that it refers to debris that is within the gravitational well of a celestial body. At this moment in time, the debris over which there is concern is, admittedly, orbiting the Earth, so the term 'orbital' is certainly applicable. However limiting concern over debris to that orbiting the Earth is arguably symptomatic of short-term thinking. Man-made debris is present in other parts of the solar system, including the satellites intentionally crashed into the Moon in December 2012 (Amos, 2013c) and the various rover missions to Mars that have since ceased to function. Of course, these defunct rovers and exploratory scientific missions are not hazards to satellites orbiting the Earth, but it is important to remember that man-made debris is not restricted to Earth-orbiting objects. Consequently, in the context of this thesis, the term ‘space debris’ is considered more appropriate, both in the short-term and, should human exploration extend beyond the Earth’s gravitational well in the decades or centuries to come, the long-term. Although this terminological clarification does not directly impact the argument and conclusions of this thesis, the author felt it relevant to emphasise that ‘space debris’ and ‘orbital debris’ are synonymous whilst outlining the reasons for their preference of the first term.

5.2.1 Protection against space debris

As noted above, a collision between an active satellite and a piece of debris larger than 10cm would likely prove catastrophic for the satellite, while a collision involving debris between 1 and 10cm in diameter could cause severe damage. The question then turns to how satellites are being protected against this danger. Accepting the premise discussed in chapter 3 of this thesis that satellites and their services are critical infrastructures, the traditional form of security is Critical Infrastructure Protection (CIP), a reactive approach which advocates the physical protection of infrastructures and the mitigation of known threats. The velocities involved mean that complete protection of satellites is, for all intents and purposes impossible, however some shielding can be used to protect against debris smaller than 1cm in diameter. This shielding involves multiple layers of material, such as Kevlar or Nextel, which are designed to absorb the force of objects colliding with the satellite and reduce their velocity, thus protecting vital components (Centre National D’Études Spatiales, 2009). However, the addition of material to a satellite can greatly increase launch costs and thus a balance must be met between physical protection and collision risk; Wiedemann *et al*. (2004) estimate that the addition of 1mm aluminium shielding to a satellite with a mass of 1000kg would increase development costs by around $8.3 million.[57] Other methods for ensuring the safety of important components include installing them behind other, less critical components or orienting the satellite so that vulnerable surfaces face the Earth (Christian, 2003: 19).

It must re-emphasised that the methods described above may shield against debris smaller than 1cm and, in some cases reduce the damage caused by larger debris, but it is widely agreed that there is no protection against debris between 1 and 10cm in size (Centre National D'Études Spatiales, 2009; Crowther, 2002: 1241). Predictions can be made regarding the possibility of collisions with catalogued debris larger than 10cm in diameter in order to allow operators to conduct Collision Avoidance Manoeuvres (CAMs), although this requires the debris in question to have been catalogued beforehand.

The SST segment of the European SSA (SSA-SST) is a significant undertaking to counter and mitigate the risk of collision between active satellites and space debris. Given that it is concerned with the existing debris clouds, the SSA-SST is arguably contributing to preventive action on the issue of space debris, albeit in a different manner to the Code discussed in chapter 4. It remains important though, in terms of outer space security, to note that while preventive security measures may be oriented towards threats with an "objectively given existence" (Massumi, 2007: para. 5), the element of surprise is still important. Whereas the measures included within the Code are directed at reducing future debris generation, the monitoring of existing debris clouds and the compilation of a debris catalogue by the SST segment serve to provide detailed orbital trajectory information to satellite operators, with the objective of forewarning operators of impending collisions, enabling them to make avoidance manoeuvres should they feel the need to do so. It could be argued that, in terms of anticipatory security, the SST segment is seeking to enhance the statistical calculability of the danger posed by the existing space debris population. The

---

[57] This calculation was based on the US dollar's value in 2002.

focus then is on securing the present through the mitigation of surprise, although there may be further applications in the future should feasible space debris remediation technologies be developed and deployed.

ESA is not the only European agency engaged in the monitoring and tracking of space debris. National institutions and agencies have a number of radar installations capable of detecting debris orbiting the Earth. The UK Fylingdales radar, operated by the Royal Air Force (RAF), is part of the USSSN and is an example of bilateral data-sharing between the UK and US. A number of European states have similar agreements with the US, including Norway, whose GLOBOS radar was installed by the US and is also part of the USSSN. Other notable European radars include the French Monge, a 10m-wide array housed on a ship, and the German Tracking and Imaging Radar (TIRA), a 70m radar which can provide images at a resolution of 10cm (Anonymous, 2012c). In addition to the Monge radar, France is also the owner of the Grand Résau Adapté à la Veille Spatiale (GRAVES), which works in conjunction with the TIRA radar to identify objects larger than 10cm orbiting the Earth between 400 and 1000km in altitude (Gattolin, 2013). Although many aspects of outer space affairs are usually shrouded in veils of national security, as with space weather, there is substantial cooperation and collaboration amongst states and scientific communities when it comes the monitoring and tracking of space debris. This is not to say however that cooperation always trumps national security; as mentioned earlier, data concerning a number space objects catalogued by the USSSN remains classified as those objects are of military origin (European Commission, 2013a).

The EC has voiced concerns over the ageing technology and infrastructure which makes up the USSSN (European Commission, 2013a: 14), as well as the need to refine and verify unsolicited warnings of future collision risks (European Commission, 2013a: 13). Given the danger posed by space debris to European outer space infrastructures and the aforementioned inaccuracy of collision warnings originating from the US, the EC announced on February 28th 2013 that it was proposing a European SST programme supported by the EU (European Commission, 2013c: 1). On the 2nd April 2014, the European Parliament adopted a position accepting a new version of the 2013 EC text (see European Commission, 2013d) regarding the creation of an EU-led SST support framework. The Decision outlining the support framework was published in May 2014 (see the European Parliament and the Council of the European Union, 2014a).

According to the Impact Assessment accompanying the 2013 EC proposal for the creation of the European SST, EU Member States are unanimous in their agreement that an independent European SST capability is required (European Commission, 2013a). Furthermore, Member States of both the EU and ESA are in agreement that any SST programme should be led by the former (European Commission, 2013a: 22). Whilst ESA is currently managing the SWE and NEO segments of the SSA and was responsible for developing the SST segment of the Space Situational Awareness Preparatory Programme (SSA-PP),[58] the EC Impact Assessment makes it clear that EU Member States have expressed concerns that the use of military facilities and responsibility over confidential information is beyond the competence of the civilian space agency (European Commission, 2013a: 22).

The justification for the development of an EU-led SST support framework is not focused solely on the avoidance of collisions between active satellites and debris; there are additional financial and operational factors involved as well. Notably, the stated objectives of the European SST framework are:

---

[58] The SSA-PP ran between 2008 and 2012 with the objective of planning and developing precursor services for the eventual European SSA (European Commission and European Space Agency, 2010: 3).

> to contribute to ensuring the long-term availability of European and national space infrastructure, facilities and services which are essential for the safety and security of the economies, societies and citizens in Europe. [… And specifically] a) assessing and reducing the risks to in-orbit operations of European spacecraft relating to collisions and enabling spacecraft operators to plan and carry out mitigation measures more efficiently; […] b) reducing the risks relating to the launch of European spacecraft; […] c) surveying uncontrolled re-entries of spacecraft or space debris into the Earth's atmosphere and providing more accurate and efficient early warnings with the aim of reducing the potential risks to the safety of Union citizens and mitigating potential damage to terrestrial infrastructure; […] d) seeking to prevent the proliferation of space debris.

Whilst the potential for improvements concerning mitigation measures – such as CAMs – stems from European concerns regarding the reliability of information originating from the USSSN, it should be noted that CAMs can have negative effects on satellites' operational lifetimes. Undertaking a CAM uses valuable fuel reserves, which are required to maintain a satellite's orbit throughout its planned operational lifetime. Thus, reducing the fuel reserves has a direct impact upon that satellite's capability to remain in orbit. Given the costs associated with producing and launching satellites, reductions in operational lifetimes can prove to be very expensive, hence the need to ensure that mitigation measures are employed efficiently.

The last stated objective for the proposed EU-managed SST concerns the safety and security of terrestrial populations and critical infrastructures. This addresses the risk of space debris surviving re-entry through the Earth's atmosphere and causing damage to terrestrial property or infrastructures, or injuring persons on the ground. There is a similar concern regarding the danger posed to aircraft by re-entering space debris. At the time of writing there is no automatic notification system in place, and ESA disseminates re-entry information to individual state agencies with the competencies to decide whether to issue Notice to Airmen (NOTAMs) warning pilots of hazards in specific geographical areas (Anonymous, 2012f). However, the SSA-PP included re-entry prediction software, which whilst an “imprecise science”, had the capability to “produce alerts of when objects start re-enter[ing] the atmosphere, and also give a very rough estimate of where they could land on the Earth’s surface” (Anonymous, 2012f). In addition, the software “generates a NOTAM […] automatically” (Anonymous, 2012f), which if successfully implemented would conceivably expedite warnings of space debris re-entry, enhancing aviation security.

Although the European SST support framework has, at the time of writing, only recently been announced, some details are beginning to emerge as to its future architecture. For instance, although ESA is developing phase array radars (Anonymous, 2012c; 2012f), the EU-led programme will rely on existing sensors owned and operated by EU Member States to complement ESA’s dedicated systems (The European Parliament and the Council of the European Union, 2014a: L 158/299). Equally, although current plans involve only Earth-based sensors, some research is being undertaken into the practicality of sensors based on-board spacecraft (Anonymous, 2012c; 2012f) similar to those installed on EUMETSAT and Galileo satellites to monitor space weather. This proposed architecture has been the subject of criticism however; a proposal to the French Senate put forward in June 2013 – following the original EC proposals in the February of that year – reacts negatively to the EC decision to make EU Member States responsible for the maintenance and development of new sensors. The criticism of the EU-led SST framework by the Commission des Affairs Européennes is predicated upon the beliefs that the architecture, governance and budget described by the EC Communication (see European Commission, 2013a) are inadequate and focused too much on short-term results. In particular, it claims that:

> if France accepts to provide an essential tool in this sector to the European Union, should the latter not participate in the maintenance and improvement of this tool? The GRAVES radar, which has allowed France to become a major actor, is now old and its predictable obsolescence must be addressed. The military programming law envisages the modernisation of GRAVES but if is to become the principal European means of space surveillance, it is expected that it would benefit from European financing (Gattolin, 2013: 11-12, translated by author).[59]

The proposal goes on to criticise the budget allocated by the EC to the proposed EU-led SST, arguing that:

> [t]o reinforce the independence of the European Union, considering the creation of new structures complementary to existing means (for example in French Guiana or Spain) will be necessary, but it requires a higher budget

---

[59] The original text reads: "si la France accepte d'apporter un outil essentiel en ce secteur à l'Union européenne, celle-ci ne se doit-elle pas de participer à l'entretien et l'amélioration de cet outil? Le radar GRAVES, s'il a permis à la France d'être un acteur majeur, est désormais assez ancien et ses obsolescences prévisibles doivent être traitées. Certes, la loi de programmation militaire envisage une modernisation de GRAVES, mais s'il doit devenir le principal moyen européen de surveillance de l'espace, il est normal qu'il bénéficie de financements européens" (Gattolin, 2013: 11-12).

> than that envisaged by the European Commission (Gattolin, 2013: 12, translated by author).[60]

Lastly, although it acknowledges that there is a degree of confidentiality involved with outer space surveillance given the military technologies and assets involved (p. 13), the Commission des Affaires Européennes, calls for the establishment of a civilian space surveillance programme (p. 18). These criticisms were reviewed and agreed upon by the French Sénat, which passed a resolution in July 2013 expressing concern that the proposed budget for the EU-led SST is insufficient and may draw funds away from the Galileo and Copernicus programmes (Sénat, 2013: 3). Furthermore, the resolution affirms the French support for the creation of a civilian SSA programme (p. 3) and advocates cooperation between France and Germany over the issue of confidentiality of military data and information gathered by their respective space surveillance capabilities (p. 4). In essence then, the French proposals by the Commission des Affairs Européennes and the Sénat are advocating a return to an architecture and governance structure similar to that of the original SSA-PP. Though this may only be the reaction of one EU Member State, the French contributions to European space surveillance capabilities through its GRAVES and Monge radars, not to mention its political influence in the region, mean that the reaction should not be ignored.

The new version of the EC's proposed decision approved by the European Parliament and the Council of the European Union in April 2014 appears not to address the majority of the French concerns mentioned above. Notably, in terms of finance, the new

---

[60] The original text reads: "[p]our renforcer l'indépendance de l'Union européenne, envisager la création de nouvelles structures, complémentaires des moyens existants (par exemple en Guyane ou en Espagne), serait nécessaire, mais elle impliquerait un budget plus important que celui envisagé par la Commission européenne" (Gattolin, 2013: 12).

text retains the position that “[t]he SST support framework should not provide financial support for the development of new SST sensors” (The European Parliament and the Council of the European Union, 2014a: L 158/299), although it does acknowledge that “[i]f a need for new sensors arises in order to meet user requirements, that need could be addressed either nationally or through a European research and development programme, where appropriate” (The European Parliament and the Council of the European Union, 2014a: L 158/299). The new text also emphasises that the development of new sensors should only take place after existing national SST assets have been networked to provide an EU-SST capability; this is unlikely to assuage French concerns over its ageing GRAVES system (see Gattolin, 2013: 11-12). Regarding the financing of the SST support framework itself, the new text continues to call for funds – with a proposed budget of €70 million – to be drawn from the Horizon 2020, Galileo and Copernicus programmes (The European Parliament and the Council of the European Union, 2014a: L 158/230). Again, this was an issue of a concern for the French Sénat (2013: 3) which appears not to have been addressed.

It is important to note that the Decision of the European Parliament and the Council of the European Union outlines the creation of a SST support framework, rather than an SST programme itself. Consequently, as mentioned above the “SST support framework shall not cover the development of new SST sensors” (The European Parliament and the Council of the European Union, 2014a: L 158/231) but will be involved in “the establishment and operation of a sensor function consisting of a network of Member State ground-based and/or space-based sensors, including national sensors developed through ESA, to survey and track space objects and to produce a database thereof” (p. L 158/231). The framework will also include the “the establishment and operation of a processing function to process and analyse the SST data at national level to produce SST information and services for transmission" (p. 158/231) to a range of stakeholders. The SST support framework will therefore cover the compilation, processing and dissemination of data collected by SST sensors but not the operation of those sensors.

The use of an SST segment and other radars to monitor and track space debris offers satellite operators forewarning in the event that a collision with their spacecraft and a piece of debris may be a possibility. However in terms of anticipatory security measures, the SST is purely preventive; it does not actively mitigate the generation of debris and only deals with dangers that exist at the present moment. In other words it is operating upon a threat with an "objectively given existence" (Massumi, 2007: para. 5). Additionally, as mentioned above, pieces of debris smaller than 10 cm in diameter cannot be tracked, although some radar arrays have the capability to detect them as they pass overhead (Anonymous, 2012f). These issues mean that the SST segment of the European SSA is, like the installation of protective shielding and component positioning, only part of the solution to the issue of space debris. However, these measures and initiatives only address the dangers posed by the existing debris population. Other alternatives must be sought for the security of outer space infrastructures to complement situational awareness and physical protection measures; namely, actions intended to limit debris generation and reduce existing debris populations. It should be noted though that if and when space debris remediation technologies become operational, SSA programmes and the data contained within debris catalogues will most likely be integral to the remediation process through the identification and tracking of large pieces of debris for de-orbiting or re-orbiting.

5.2.2 Space debris mitigation and remediation

There is currently no legally-binding international law on the topics of space debris, its generation and its mitigation or removal. Although the United Nations Committee on the Peaceful Uses of Outer Space (UNCOPUOS) has been debating the issue for some years, the first substantial document did not emerge from the UN until 2007, with the endorsement of the UN Space Debris Mitigation Guidelines, a set of guidelines based upon those published by the IADC in 2002 and revised in 2007 (see Inter-Agency Space Debris Coordination Committee, 2007). Space debris, like many other issues relating to the human exploration and exploitation of outer space, is a controversial issue. On the one hand, most, if not all, state and non-state satellite operators recognise the risks posed by space debris. However, space debris can be generated in a number of ways, some of which some states are not keen on preventing. In particular, the development of ASAT technology has proved to be a stumbling block, with the US maintaining its right to the future research and development of systems which can be used to protect its assets in outer space (see White House, 2006; 2010b). Additionally, as Robinson (2012) argues, "[a]lthough most countries agree that an arms race in space is not desirable, there is no consensus that such an arms race is underway, and hence no [perceived] need for […] arms control measures". Consequently, current efforts to curb the growth of space debris orbiting the Earth revolve around national and international mitigation guidelines. While international guidelines, such as the UN Space Debris Mitigation Guidelines, are not legally-binding, they do establish a set of recommended practices for states and organisations engaged in the exploration and exploitation of outer space. National guidelines are, though, arguably more effective, as they are enforced by the government which created them upon all space missions developed within that state.

5.2.2.1 Space debris mitigation

Attempts to mitigate the generation of space debris tend to revolve around good practice on behalf of the manufacturers and operators of launchers and satellites. Some measures are perhaps more obvious than others; for example ensuring launchers or satellites do not fragment or that components do not break away from their host whilst operational. However a lot of emphasis has been placed on the passivation of fuel tanks, a process which involves leftover fuel being expelled from the tanks at the end of a space object's operational lifetime to avoid combustion and the resulting fragmentation of the object. Accidental collisions between space objects are also of concern and on this matter, the UN Space Debris Mitigation Guidelines require that "the probability of accidental collision with known objects during the system's launch phase and orbital lifetime should be estimated and limited" (United Nations Office for Outer Space Affairs, 2010: 3).

The IADC Space Debris Mitigation Guidelines propose the establishment of two protected regions in which any activities should be undertaken with close concern for the generation of space debris. These regions are LEO, up to an altitude of 2,000km, and the area spanning 200km and 15 degrees of latitude above and below GSO (Inter-Agency Space Debris Coordination Committee, 2007: 6). LEO and GEO/GSO are recognised as being the most densely populated orbital regions, hence the attention to the promotion of sustainability in these specific areas.

With regards to the post-operational disposal of satellites, the common recommended practice involves the de-orbiting and re-orbiting of satellites just before their operational life ends. These practices are commonly associated with satellites located in densely populated orbital altitudes, such as LEO and GEO, where obsolete objects could be occupying valuable physical space or could prove a danger to other active objects as their orbits slowly degrade. As noted above, this also the reason that these regions have been designed protected areas by the IADC. Satellites based in LEO are often de-orbited to re-enter the Earth's atmosphere, a journey intended to result in the destruction of much of the object in question. Nonetheless, it should be noted here that fuel tanks or other sturdy components often survive re-entry and fall to the surface of the Earth.[61] Although these components tend to land in oceans or sparsely populated regions (Ailor and Patera, 2007), there have been some incidents where limited damage has been caused to property, requiring compensation from the operator of the satellite from which the component originated. As with collisions in outer space, the state under which the satellite is registered is liable for the compensation, as per the 1972 Liability Convention. The first, and thus far only, application of the Liability Convention occurred after Kosmos 954 re-entered the Earth's atmosphere over Canada in 1977 (Shaw, 2003: 483). The satellite had suffered an on-orbit malfunction which resulted in its operators being unable to control its altitude or eject its nuclear core into a disposal orbit. Some radioactive debris from the satellite survived re-entry and was spread out over a distance of 600km. The incident was eventually resolved through diplomatic negotiations without the need for independent arbitration (Listner, 2012a) but serves as a reminder of the danger space debris can pose to the Earth's surface.[62]

Unlike satellites in LEO, spacecraft in GEO/GSO do not re-enter the Earth's atmosphere as the distances involved are too vast. Instead, they are re-orbited to what is known as a graveyard orbit, located above GEO but far enough away to avoid collisions between active and other re-orbited satellites. This practice, whilst thus far successful in avoiding collisions in the protected zone of GEO is nonetheless creating a field of debris which will likely remain in orbit for thousands of years. Until effective remediation measures are developed, these obsolete satellites will continue to orbit the Earth and slowly

---

[61] It has been estimated that between 10-40% of a satellite's mass will survive re-entry, although very little is ever recovered from the Earth's surface (Ailor and Patera, 2007: 947).

[62] Under Article 2 of the Liability Convention, "[a] launching State shall be absolutely liable to pay compensation for damage caused by its space object on the surface of the Earth or to aircraft in flight" (United Nations, 2002: 13). With regards to damage caused elsewhere – in outer space for instance – Article 3 of the Liability Convention states that a launching state "shall be liable only if the damage is due to its fault or the fault of persons for whom it is responsible" (United Nations, 2002: 14).

fragment. Although the resulting debris may not be an urgent threat to active satellites, questions must be raised about the ethics of deliberately generating debris fields for future generations to deal with. Existing international and national standards, such as those of NASA, only establish the distances which must be maintained between the protected zone of GEO and these graveyard orbits (see National Aeronautics and Space Administration, 2009: 22; United Nations Office for Outer Space Affairs, 2010). Returning to the precautionary principle found in arguments surrounding anticipatory security measures (see chapter 3 of this thesis), although the possibility of overcrowding in graveyard orbits is for the time being purely hypothetical, it is necessary to consider the implications of the Kessler Syndrome emerging above GEO. The creation of debris fields above GEO could be hazardous to operations in the region, particularly if orbits degrade to the extent that perigees eventually breach the protected zone. Nonetheless, current technological limitations mean that the re-orbiting of satellites in GEO is the only recourse available at the end of their orbital lifetimes, and consequently the ethical ambiguity of this practice serves only as a reminder of the continuous, and most likely permanent, pollution of the extra-terrestrial environment being undertaken to support terrestrial societies.[63]

From the guidelines and measures mentioned above, it should be clear that although states are liable for the satellites that are registered under their flag, the onus is firmly with the satellite manufacturers and operators to limit debris generation. States are thus responsible for ensuring that the manufacturers and operators for whom they have registered satellites are adhering to the various international obligations that exist concerning space debris and overall good practice in outer space activities. This is largely

---

[63] The possibility exists for graveyard orbits to expand beyond their primary function and contribute to outer space archaeology. Idziak (2013) contends that with appropriate planning and management, “orbital preservation cluster positions and altitudes” (p. G:72) could be established to maintain records of the development of spaceflight for future generations.

undertaken through national space policies and debris mitigation standards, although some national space agencies have cooperated to create guidelines which reflect agreed practices, such as the European Code of Conduct for Space Debris Mitigation.

Although the problem of space debris came to the attention of satellite operators and policy-makers after around 30 years of space exploration and exploitation (Crowther, 2003), the first mitigation standards did not appear until 1995, when NASA published the NASA Safety Standard Guidelines and Assessment Procedures for Limiting Orbital Debris.[64] This standard was replaced by the NASA Technical Standard Process for Limiting Orbital Debris, published in 2007 and recently updated in 2009. While they apply only to NASA missions, the standards are nonetheless indicative of the risk space debris is perceived to pose and of the measures that can be taken to avoid its generation. Importantly, these measures are, as of the 2009 NASA Standard, requirements rather than simple guidelines (Johnson and Stansbery, 2010: 364), a change which, even if only procedural, highlights the severity of the issue at hand.

Given the variations in orbital lifetimes between orbits of differing altitudes, debris generation for missions passing through or operating within LEO and GEO are treated separately within the 2009 NASA safety standard. Requirements 4.3-1 and 4.3-1a establish that “[f]or missions leaving debris in orbits passing through LEO […] [a]ll debris released during the deployment, operation and disposal phases shall be limited to a maximum orbital lifetime of 25 years from the date of release” (National Aeronautics and Space Administration, 2009: 22). Meanwhile, requirement 4.3-2 states that:

---

[64] It should be noted that although the first NASA policy on space debris – NASA Management Instruction 1700.8 – was published in 1993 (Johnson and Stansbery, 2010: 362), the 1995 guidelines were the first formal assessment of the generation of space debris conducted by NASA.

> [f]or missions leaving debris in orbits with the potential of traversing GEO (GEO altitude +/- 200 km and +/- 15 degrees latitude), released debris with diameters of 5cm or greater shall be left in orbits which will ensure that within 25 years after release the apogee will no longer exceed GEO - 200 km (National Aeronautics and Space Administration, 2009: 22).

It should be noted that as all missions to GEO must pass through LEO, they must also adhere to requirement 4.3-1 and its subsequent clauses.

The 2009 NASA safety standard is, unsurprisingly, more comprehensive and detailed than its 1995 precursor, reflecting many subsequent developments in policy-making and research. One example of note pertains to debris generation around GEO; the 1995 document requires that any debris generated should, within 25 years, not have a higher apogee than 300km below GEO (National Aeronautics and Space Administration, 1995: 12). Compared to the 2009 document quoted above, which recommends an apogee no higher than 200km below GEO, there has arguably been a significant reduction in the protected area around GEO. The 1995 safety standard required a 300km protection zone below GEO in an attempt to “prevent the development of a significant debris environment, as currently exists in LEO” (National Aeronautics and Space Administration, 1995: 13). The reason for this reduction is, as explained in the 2009 safety standard, that:

> In 1997 the IADC […] completed a detailed study of GEO with an objective of developing a requirements-based recommendation for the disposal of space structures near GEO. The IADC concluded that a region within 200 km of

> GEO be preserved for the operation and relocation of GEO spacecraft (National Aeronautics and Space Administration, 2009: 41).[65]

This example is illustrative of the ever-developing nature of outer space affairs. Although space exploration and exploitation has been nearly constant since 1957, knowledge and understanding of extra-terrestrial environmental factors is still growing. Consequently, it must be remembered that all space debris mitigation guidelines and recommendations for best practices are based upon current – and relatively short-term in comparison to the orbital lifetimes of some debris – research.

NASA is not the only national space agency, and by association the US not the only state, to have published space debris mitigation guidelines. In Europe, ESA published space debris mitigation guidelines in 2008, which following the example set by the IADC, designates LEO and GEO as ‘protected regions’ (European Space Agency Director General’s Office, 2008: 6). Consequently, any ESA mission must ensure that any debris generated during missions should not detach from the spacecraft. However, if the debris must separate from the spacecraft, Design Requirement-02 of the guidelines states that said debris must not enter into the GEO region and must not remain within LEO for longer than 25 years (European Space Agency Director General’s Office, 2008: 5). It is also notable that with reference to the Copernicus programme, the European Parliament and the Council of the European Union (2014b) explicitly requires the “safe decommissioning of the [Sentinel] satellites at the end of life” (p. L 122/53).

Individual European states also have their own national approaches to outer space activities, including the issue of space debris. To take the UK as an example; although it

---

[65] The reduction of size in the protection region around LEO is also reflected in the IADC Space Debris Mitigation Guidelines (Inter-Agency Space Debris Coordination Committee, 2007: 6).

does not have a specific space debris policy, the 1986 Outer Space Act outlines the conformity of UK legislation with regards to international law concerning outer space activities. As part of the Outer Space Act, all entities in the UK, its Overseas Territories or its Crown Dependencies wishing to launch or operate satellites must obtain a license from the UKSA on behalf of the UK government (Anonymous, 2012d; United Kingdom Space Agency, 2013). This license grants licensees the right to launch and operate satellites on the condition that those operations do not infringe the UK's international legal obligations, affect the national security of the UK, interfere with other entities' activities in outer space or, last but not least, contaminate either the outer space or Earth environments (*Outer Space Act*, 1986: 5.-2e). A license can be revoked, altered or suspended at any moment if it appears that the requirements of said license have not been adhered to, or if it is necessary for the sake of public health or national security (*Outer Space Act*, 1986: 5.-2). In addition to the regulation of licenses, the UK government is required to maintain a register of space objects owned or operated by UK entities (*Outer Space Act*, 1986: 7.-1) in compliance with the 1976 Registration Convention.

The 1986 Outer Space Act does not include any specific mentions to space debris, however a number of conditions placed upon licensees arguably requires the limitation of debris generation. Of particular relevance here are the conditions concerned with avoiding liability for damage caused to other objects and ensuring that the outer space environment is not contaminated. As the launching state for satellites owned by UK-registered entities, the UK is liable for any damage they cause under the 1972 Liability Convention. Applicants for UK licenses must provide a risk assessment including possible failures, any conceivable effects of those failures and the risks associated with the launch and operations of their satellite (Portelli *et al*., 2010: 1037). Moreover, it could be argued that the condition requiring licensees to ensure that operations do not interfere with the activities of other satellites applies to all forms of interference, including collisions and radio frequency overlaps. The approval of an application is determined based upon existing international standards and guidelines for outer space activities, including IADC recommendations and the UN Space Debris Mitigation guidelines (Anonymous, 2012d; Portelli *et al.*, 2010: 1038). Also included within the list of reference documents is the European Code of Conduct for Space Debris Mitigation, a document drafted and signed by the space agencies of France, Germany, Italy and the UK in 2004, as well as ESA in 2005. The Code of Conduct includes a host of provisions aimed at reducing the generation of space debris during and after active operations.

France is another pertinent example of the efforts undertaken by European states to deal with the issue of space debris. Like the UK, France does not have a specific space debris policy so to speak, although all new projects associated with the French Centre National d'Études Spatiales (CNES) must adhere to the European Code of Conduct for Space Debris Mitigation. The practice of doing so has revealed that some smaller launchers and satellites which began operating before 2004 struggle to comply with this Code of Conduct, particularly with regards to de-orbiting from LEO within a period of 25 years (Portelli *et al.*, 2010: 1039). Moreover, and with particular relevance to the Galileo and Copernicus programmes, the French Loi n° 2008-518 du 3 Juin 2008 relative aux opérations spatiales applies to all launches from territory under French jurisdiction or by a French company. As Arianespace is a French company launching from a French overseas territory, this law thus applies to its launcher operations. Pursuant to France's international obligations, under Article 12 of this law CNES is responsible for maintaining a registry of all objects launched by French companies or from French territories (République Française, 2013). Regarding the generation of space debris and in accordance with Article 3 of the Liability Convention (United Nations, 2002: 14), Article 13 of Loi n° 2008-518 establishes that operators are held responsible for any damage caused to persons or objects on the ground or in the air but are only accountable for extra-terrestrial damage where fault can be established (République Française, 2013). Although, like the UK's Outer Space Act, there is no explicit reference to existing space debris mitigation guidelines or standards, it is expressed in Article 5 that:

> [t]he authorisations delivered in application of the present law may be accompanied by requirements enacted in the interest of the security of persons and property and public and environmental health, notably with respect to limiting the risks linked to space debris (République Française, 2013, translated by author).[66]

5.2.2.2 Space debris remediation

Space debris remediation efforts are focused upon space objects which are considered 'non-responsive', insofar as they cannot be controlled by commands from Earth. This classification includes obsolete satellites or launch vehicles which have run out of propellant, as well as fragments from man-made objects. While space debris remediation technologies are being actively researched and developed, no non-responsive objects in space have thus far been de-orbited or re-orbited.

Existing proposals for debris remediation methods include drag augmentation technologies – designed to expand the cross-section of a space object increasing the atmospheric or solar wind drag that it is subjected to – and tugs designed to attach

---

[66] The original text reads: "Les autorisations délivrées en application de la présente loi peuvent être assorties de prescriptions édictées dans l'intérêt de la sécurité des personnes et des biens et de la protection de la santé publique et de l'environnement, notamment en vue de limiter les risques liés aux débris spatiaux" (République Française, 2013, 2013).

themselves to a space object via use of a harpoon system (Amos, 2012d) or net before de-orbiting or re-orbiting it. Research and development into these methods is being undertaken by both scientific and academic institutions. ESA’s Clean Space initiative for example, whilst looking towards the environmental impacts of outer space activities both on Earth and in outer space, includes the development of space debris remediation technologies as one of its primary concerns (European Space Agency, 2013b).

As an anticipatory security mechanism, space debris remediation is speculative yet urgently required. Predictions for future debris generation indicate that large space objects will need to be de-orbited from LEO at a rate of 10-15 per year in order to avoid onset of the Kessler Syndrome (Klinkrad, 2013: 18). However, the choice of which objects to target will be largely speculative, albeit directed towards those located in densely populated orbits. Some objects may be more obvious targets that others; for instance satellites in LEO which suffer technical failures meaning that they are expected to have uncontrolled decaying orbits – ESA’s Envisat being a prime example – pose a danger to other outer space activities. In addition, booster stages for GEO/GSO satellite missions may well not have been passivated, making them dangers to other objects with nearby orbits. With regards to GSO, obsolete satellites which have not been re-orbited occupy valuable orbital slots and with time may begin to lose their position, also threatening nearby satellites. Although the space debris situation in GEO/GSO is not as severe or urgent as in LEO, long-term remediation strategies and technologies are nonetheless required given the financial and practical value of the orbital region.

Despite the urgency associated with the issue, there are legal obstacles alongside the technological ones. Space debris – including obsolete satellites and fragments – remains under the ownership of the entity which launched it. That debris cannot be intentionally influenced without the consent of the owning state. Furthermore, additional liabilities would be introduced by debris remediation undertaken by an entity other than the launching state; for instance, it would have to be established whether the de-orbiting entity or launching state would be liable for any damage caused by de-orbited debris on the surface of the Earth or to aviation in flight. Another issue with many existing space debris remediation proposals is their potential for misuse. Taking the Astrium ‘harpoon’ system as an example, which is designed to pierce an obsolete satellite before de-orbiting it (Amos, 2012d), the problem lies in that the technology could be easily used as an aggressive weapon against active satellites. Given these legal obstacles, there needs to be a comprehensive governance structure in place accounting for liabilities and responsibilities before space debris remediation can take place.

5.3 Resilience in European outer space activities

As mentioned in chapter 3, with regards to the security of terrestrial critical infrastructures, measures associated with CIP are now commonly seen as being part of a larger approach known as Critical Infrastructure Resilience (CIR). However, the efforts detailed above undertaken by the EU and satellite manufacturers to protect outer space infrastructures from NEOs, SWEs and space debris could be conceived of as being closer to CIP than CIR; they are arguably largely attempting to negate the threats rather than planning for scenarios where catastrophe occurs. From a wider perspective of outer space security, the protection of infrastructures through the mitigation of possible vulnerabilities fits with what Baines (2004) terms ‘passive defence’. According to Baines, “[p]assive defences include employing information assurance, electronic protection and weapon effects hardening. Space systems are also protected by dispersion, redundancy, reconstitution and avoidance strategies” (pp. 151-152). From Baines’ description, it would appear that the focus of ‘passive’ outer space security is split between mitigation, protection and resilience, an account supported by Cooper's (2003) analysis of the US military doctrine of 'responsive space'; "the ability to replace failed satellites quickly, to re-attempt a launch after an aborted try, and to respond to operational requirements to satisfy national security interests" (p. 44). One of the most common methods of introducing resilience into a system is redundancy, yet with the exception of GNSS constellations and some telecommunication networks very few operators maintain backup components or satellites in case of failure.

Since launching and maintaining satellites is an expensive affair, for financial reasons in-orbit backup satellites are often impractical unless part of the mission's operational requirements. Although backups can be kept in storage on Earth, ready should there be a catastrophic failure of an operational satellite, it was estimated in 2002 that these can take between four and six months to be launched (US General Accounting Office, 2002: 23).[67] The reason for the delay is often due to the time necessary to procure a launcher and organise the relevant registration documents. With regards to the registration documents, the UKSA for instance, recommends applicants for UK satellite licences begin their application at least six months before they intend to launch (United Kingdom Space Agency, 2013).

Both the Galileo and Copernicus programmes have satellite redundancies in their mission design. Galileo, like GPS, will most likely offer a guaranteed service based upon a set number of operational satellites, although a number of backups will be in orbit in case of malfunction or repair. At the time of writing, only six Galileo satellites have been launched – and of those only two are classified as having Fully Operational Capability (FOC) – so this redundancy does not yet exist, however the programme's design calls for

---

[67] The capability to launch satellites necessary for terrestrial force multiplication in "days or weeks" is an objective of the on-going US Operationally Responsive Space initiative (Operationally Responsive Space Office, 2013).

30 satellites while only 24 are required to provide a guaranteed service (Clark, 2014). Once all 30 satellites have been launched there will therefore be six satellites offering on-orbit redundancy in the event of malfunction. The Sentinel missions for Copernicus on the other hand, are designed to be comprised of either two or three satellites and thus although the failure of one of them would reduce the efficiency of the mission, the remaining satellite(s) could feasibly compensate (Anonymous, 2013).

Redundancy within a satellite can be achieved through the installation of backups for critical components, although once again this is an expensive process given the exponential increase in launch costs for extra weight added to payloads. Nonetheless, the 2002 US General Accounting Office report into the security of commercial satellites notes that US commercial operators often include redundant components "to ensure survivability", even if complete hardware redundancy is uncommon (p. 23). Such redundancy is an important factor in ensuring the continued operations of a satellite where there is risk of exposure to radiation or collisions with space debris.

As discussed in chapter 3, Scalingi (2007) defines a resilient infrastructure as "*a component, system, or facility that is able to withstand damage or disruption, but if affected, can be readily and cost-effectively restored*" (p. 51, original emphasis). Following the measures discussed above, it can be argued that the redundancy that will be present within the Galileo constellation will mean that most damage or disruption to individual satellites would not have a disastrous affect upon the programme's services as a whole. However, the time taken to develop, construct and launch the Galileo satellites indicates that in the hypothetical event of a failure of one or more satellites, replacements could not be launched soon. Moreover, from information available in the public realm it is unclear how the Galileo programme would cope in the event of a constellation-wide software failure similar to that suffered by GLONASS in April 2014 (see Cameron, 2014).

Nonetheless, given the redundancy that will eventually exist within the Galileo programme the argument can be made that it will have a high degree of resilience once fully operational.

In terms of the Copernicus programme, as mentioned above there should be some redundancy in place once all the satellites have been launched. However the satellites for each Sentinel mission will not always be launched simultaneously; as an example, ESA is planning to launch the Sentinel-1B satellite in 2016, two years after its sister satellite Sentinel-1A (European Space Agency, 2014a). As discussed with regards to anticipatory security measures in chapter 3, contingency scenarios and simulations are often run to condition those working a particular field on how best to react to a given situation. At the time of writing, it would appear that at least as far as Copernicus it is concerned, there are no plans for contingency scenarios by the EC in the event of a complete satellite failure or loss of signal from one or more of the Sentinels (Anonymous, 2013). It can be assumed therefore that the EC considers the inherent redundancy of the multiple-satellite missions sufficient to accommodate for any malfunctions or failures. However, the malfunction of Envisat in 2012 exists as a reminder that should all the Sentinels dedicated to a particular mission malfunction or fail, replacement satellites may well take months or years to be built and launched. Admittedly, the EC would be relatively powerless in the event that all the satellites of a particular Sentinel mission fail but the absence of contingency scenarios is striking nonetheless.

5.4 The astro- and geopolitics of the European SSA and SST programmes

As discussed above, the SSA or any European system dedicated to the monitoring of space debris, space weather and NEOs relies upon a network of sensors located across a wide geographical region. Prior to the SSA-PP individual states undertook their own space surveillance, commonly using military systems and sharing data through bilateral agreements (Anonymous, 2012f). In addition to the benefits provided by the pooling of resources, a multi-actor SSA programme represents a coordination of data-sharing amongst those actors. As the US currently maintains the most comprehensive SST programme and space object catalogue, much of the information shared with regards to space debris originates from there (Anonymous, 2012c; European Commission, 2013a). It could be argued therefore that the USSSN is an example of ‘soft’ power projection, established through the control that the US maintains over the dissemination of information obtained through its space surveillance capabilities.

The concerns voiced by the EU and its Member States regarding the confidentiality of data and installations associated with the proposed European SST point to the wider complexities of outer space security. On the one hand, data compiled by any SST or SSA programme needs to be disseminated, but the process through which that information is obtained depends largely on military capabilities requiring high levels of confidentiality and security. The dissemination of information is crucial; creating catalogues of data relating to the size, shape and orbital paths of space debris means very little if satellite operators are not given the opportunity to use that data. Consequently, there needs to be a robust yet effective data policy with regards to the proposed European SST, and indeed it appears that this is an issue that both the EU and its Member States are aware of (see European Commission, 2013a). At the time of writing, it remains unclear what the specific restrictions imposed by an SST data policy will be but the Impact Assessment associated with the draft SST proposal states that "[u]nder any scenario, [an] SST data policy must upheld [*sic*] the principle that information is by definition classified and it should only be declassified on a case by case basis when the need arises" (European Commission, 2013a: 23). The need for confidentiality when it comes to the military facilities, activities and information gathering practices of Member States is not subject to debate here, however the assertion that data "should only be declassified on a case-by-case basis when the need arises" (European Commission, 2013a: 23) is concerning, as it allows for the possibility of variations in what is considered an acceptable 'need'. The Impact Assessment does comment upon the requirement for what it terms a 'front desk function' dedicated to SST data dissemination and comments that from discussions with EU member states, the preferred means of achieving this is through entrusting the role to an existing organisation "with a record as service provided and suitable credentials in the security domain, such as the European Union Satellite Centre" (European Commission, 2013a: 40). However, it should be noted that the French Sénat resolution on the proposed EU-led SST objects to the inclusion of the European Union Satellite Centre within the programme (Sénat, 2013: 4), indicating that there is disagreement over the future SSA data policy.

Should the dedicated European SST programme come to fruition, it would arguably represent a significant enhancement of European outer space capabilities. With respect to the EU's ambitions for leadership in outer space affairs, a network of upgraded sensors, processing centres and dissemination practices would most likely position Europe as, at the very least, a competitor to the US in terms of the detection and tracking of space objects, particularly given the ageing infrastructure of the USSSN. Moreover, as the February 2013 proposals for the EU-led SST establish that sensors will remain under the management of the respective Member States which currently operate them, the programme would be an example of European coordination and collaboration across institutional and national levels.

Stepping back to a wider astropolitical perspective of SSA programmes, the capability to monitor and track objects in near-Earth space arguably runs the risk of transforming how the materiality of the region – and with it the materiality of outer space security – is conceived. As reliance upon SST sensors increases, near-Earth space may well metamorphose from a 'material', 'real' domain into a virtual catalogue of 'safe' and 'unsafe' objects, whereby the safety of said objects is determined by their operational status and the statistical probability of collisions. The region is no longer a space of astrophysical forces but a host of dangers, vulnerabilities and objects requiring protection. This has already taken place to an extent, with space debris being applied as a blanket term to any non-operational man-made objects in outer space. Operational objects are, by and large, considered 'safe' as their trajectories can be manipulated by their terrestrial operators, whilst obsolete and fragmented objects are 'unsafe' threats *in potentia*. The inability of anyone to control these 'unsafe' objects necessitates the development and use of SST sensors to protect the 'safe' objects, and by association the services they provide, through advanced warning of possible collisions. In effect, awareness and statistical probabilities are being used as a substitute for a capability to influence the 'unsafe' objects and the dangers they pose. As de Montluc (2012) notes, with the exploration and exploitation of outer space likely to increase in the future, "[s]uch surveillance might in fact become a precondition of our capability to access space on acceptable security/safety terms and to conduct operational activities" (p. 199). It is even possible, if not likely, that the potential future importance of the SSA to outer space activities means that it soon becomes considered as a critical infrastructure itself.

In addition, the active compilation of space object catalogues by actors with SSA capabilities is arguably representative of a statistical cartography of near-Earth space and its material population. Such catalogues bear similarities to what Dodds (2008; 2010b) describes as US efforts to make the seabed of the Arctic Ocean "legible" (2010b: 66) during the second half of the 20th Century. Just as the US was intent on monitoring and tracking Soviet movements in the Arctic, cataloguing actors desire to monitor and track space objects, both active and inactive or fragmented. Although the primary justification for such catalogues may be to anticipate possible collision risks between objects, they serve a secondary purpose of mapping near-Earth space with the trajectories of space objects being the points of reference. This cartographically-enabled ‘legibility’ complements the aforementioned categorisation of space objects as ‘safe’ and ‘unsafe’ bodies, furthering the emerging bipolar subjectivity of materiality in near-Earth space.

5.5 Extra-terrestrial environmental security and the security of critical infrastructures

Understandably given the importance of satellite constellations, there is a high level of confidentiality associated with outer space security and few, if any, details of the protection technologies or the threats being protected against are available in the public sphere. Nonetheless, some trends can be gleaned from general recommendations and standards, such as those published by the CCSDS, the IADC, the UN and national space agencies. The common approach to environmental risks and dangers is one of anticipatory mitigation through those general recommendations and standards advocating ‘good practice’. In terms of Europe, the focus of the European SSA on space weather and space debris arguably indicates the environmental dangers the EU perceives to be most threatening to its outer space segments.

Radiation has the potential to cause significant interruption to operations of outer space critical infrastructures. It originates from both existing belts around the Earth, known as the Van Allen belts, and from space weather phenomena. SWEs, which include CMEs, charged energetic particle bursts and solar flares, produce two forms of radiation; electromagnetic and energetic particle radiation. As the occurrence of SWEs cannot be prevented, protection efforts turn towards resilience through forewarning and hardware design. The forecasting of SWEs already takes place on a global scale involving international cooperation and collaboration amongst scientific communities, although Europe is in the process of attempting to improve its regional coordination through the inclusion of SWE monitoring in its SSA programme. When framed within an anticipatory security perspective, the focus on forecasting and forewarning means that the SSA-SWE segment is both preemptive and preventive in its approach to the risks and dangers posed by radiation originating from space weather phenomena. The research being undertaken into large SWEs on a scale similar to the Carrington Event is particularly precautionary as the overall objective of this research is to mitigate to some extent the surprise at the nature and potency of the event should one occur in the future.

The design of satellites to mitigate the effects of radiation upon electronic components and other hardware through hardening is arguably a form of protection along the lines of physical security advocated by CIP recommendations. It is designed to protect the critical components of a satellite from a danger that is partially unknown. Moreover, this protection is the last line of defence, so to speak; it is complemented by hardware redundancy and the ability of satellite operators – following forewarning from those monitoring SWEs – to manoeuvre operational assets so that vital electronics are not directly hit by waves of radiation following those events. Together, these practices and design features introduce resilience into satellite operations, working to compensate for the uncertainties of the effects of radiation upon satellites and their components, and are thus arguably representative of an anticipatory logic.

With regards to space debris, there is a similar introduction of resilience through design and forewarning. The use of shielding on satellites to protect vital components from debris and other space objects alongside hardware redundancy – of both components and, in some situations, satellites – mean that collisions with space debris smaller than 10cm are not necessarily catastrophic. In addition, warnings from actors with space surveillance capabilities – such as the USSSN and eventually the European SST – enable satellite operators to undertake CAMs in order to avoid possible collisions between their outer space assets and debris or other space objects. Again, these measures are relatively preventive in their approach to the security of outer space infrastructures as they are directed at avoiding the surprise of the occurrence of a relatively clear and imminent danger. As with the USSSN, the role of the European SST will be to compile a catalogue of existing space debris, monitor the debris populations and provide detailed orbital trajectory information to satellite operators, with the objective of forewarning operators of impending collisions. It is therefore primarily dedicated towards the imminent and extant risks and dangers posed by the existing space debris population rather than the long-term population growth.

There is an element of preemptive thinking however within the numerous space debris mitigation guidelines and standards. Although these are not specific to Europe or the EU, ESA has published its own guidelines (see European Space Agency Director General’s Office, 2008) and the Code advocates adherence to the UN Space Debris Mitigation Guidelines (European Union, 2013: 4-5). Whilst these guidelines are focused on the short-term mitigation of space debris generation, they nonetheless represent a preemptive and precautionary approach to the long-term sustainability of outer space activities. The possibility that space debris will begin colliding with each other, causing an exponential growth in the population at some orbital altitudes, is a risk with many unknown consequences. As with research into SWEs on a similar scale to the Carrington Event, the warnings that the Kessler Syndrome may become reality have a conditioning effect, potentially reducing the surprise at the consequences of the event and perhaps even at the occurrence of the event itself.

As the main EU collaborative project concerning extra-terrestrial environmental security, the European SSA is a preemptive and preventive anticipatory security mechanism; the SST and SWE segments are predominantly oriented towards forewarning of imminent threats posed by space debris and space weather through the use of statistical probability calculations. These two segments also seek to reduce the spatio-temporal uncertainties inherent within outer space security by enabling the prediction of which space objects may be affected by a certain danger or threat. In this manner, they work to mitigate the element of surprise caused by unanticipated collisions or radiation by informing operators of significant risks, allowing them to make avoidance manoeuvres if necessary. Regarding preemptive measures, although research is being undertaken into the possibility and consequences of cascading debris generation or large-scale space weather events, it does not appear to be a central component of the European SSA. This being said, space surveillance is intrinsically a passive security mechanism focused upon existing and statistically calculable dangers and, until the technologies and governance structures are in place for space debris remediation, the SST segment will have limited application in terms of precautionary or preemptive actions other than the forewarning of impending collisions. If and when space debris remediation becomes viable it is feasible that SST programmes will be able to identify particularly hazardous debris necessitating de- or re-orbiting, but until then the absence of practical application for such data means that they will remain security mechanisms primarily dedicated to monitoring debris populations and providing collision warnings.

There is a need to remain wary of placing complete dependence upon the SSA and other space surveillance programmes. While there can be little doubt that the data they provide is integral to sustainable outer space activities – particularly if and when space debris remediation becomes commonplace – there needs to be a continued effort towards advocating space debris mitigation standards and technologies alongside practices introducing and improving resilience in critical outer space infrastructures. SSA capabilities should be considered complementary to the aforementioned mitigation standards and practices, as well as diplomatic initiatives directed at promoting sustainability in outer space.

6 Conclusion

This thesis has explored the means through which the European Union (EU) is looking to ensure the short- and long-term security of the space segments of its outer space critical infrastructures from a broadly critical constructivist perspective by exploring the risks and dangers that the EU publically perceives and constructs as being the most threatening to those space segments. This research project has defined outer space security as: ‘the secure and sustainable access to, and use of, outer space, whereby an entity is confident that any unreasonable (unjustified) dangers or risks they identify as threatening to their outer space infrastructures have been sufficiently mitigated against’. The emphasis on actor-specific risks, dangers and responses outlined through policy documents, legislation and semi-structured interviews has enabled an analysis of the EU’s unique outer space security identity. The original contribution to knowledge offered by the thesis is the framing of European outer space security as predicated upon anticipatory mechanisms targeted towards the space segments of critical outer space infrastructures. It should be noted that security in outer space is performed largely at a material, rather than astrographical, level; the highly-mobile nature of near-Earth space means that the subjects of outer space security are the infrastructures and the assets which comprise them, rather than the orbits they occupy. These infrastructures are comprised of the ground and space segments (the hardware) along with the connectivity between those segments, which includes the services that the infrastructures are providing. This thesis has focused upon the security of the space segments of the EU’s critical outer space infrastructures, although –

as mentioned later in this conclusion – there is the opportunity for future research to be undertaken concerning the security of ground infrastructures.

As outlined in the introduction, this thesis has sought to answer four questions:

1. Are outer space infrastructures critical infrastructures for the EU, and if so, why?
2. To what extent does the EU recognise this?
3. What risks and dangers does the EU perceive to be threatening to the space segments of European critical outer space infrastructures?
4. How is the EU attempting to ensure the security of the space segments of its critical outer space infrastructures against these risks and dangers, and how can this be conceptualised?

6.1 Europe, outer space and European critical outer space infrastructures

With reference to the first two questions posed in the introduction, the European Commission (EC) has identified European outer space infrastructure – by which it is arguably referring to outer space programmes and associated hardware and services – as being "critical infrastructure on which services that are essential to the smooth running of our societies and economies and to our citizens' security depend" (European Commission, 2011a: 6). As argued in chapters 2 and 3, pan-European space programmes, such as Galileo and Copernicus, offer support for terrestrial EU policies on regional and external issues ranging from improved transportation and promoting research into, and awareness of, climate change. In doing so, these programmes arguably act as mechanisms of policy-multiplication and space power projection, demonstrating the status of the EU as an independent actor in outer space affairs.

Despite this and public acknowledgements of the need to secure critical outer space infrastructures (see Council of the European Union, 2010; European Commission, 2013a), they remain excluded from the categories of European Critical Infrastructures (ECIs) (Council of the European Union 2008a: L 345/81), a label which activates legislation regarding confidential identification and security. Although an important aspect of the ECI-identification process is that such identification be confidential, chapter 3 of this thesis argues that there is a tension between the existing definition of ECIs and the nature of outer space infrastructures, in that important components including the satellites, ground segments and launch facilities, are often located across and outside of the territorial borders of EU Member States. This tension extends to some terrestrial infrastructures which often involve connectivity between their components and other infrastructures. It can be assumed therefore that, at least at the time of writing, European critical outer space infrastructures are considered separate to terrestrial ECIs, even though they provide vital services to multiple Member States.

The tension regarding the security of critical outer space infrastructures is not only a European problem. Although states and institutions may regularly refer to outer space assets as infrastructures, critical or otherwise (see Council of the European Union, 2010; European Commission, 2011a; 2013a; House of Commons Defence Committee, 2012; United States General Accounting Office, 2002), they remain ignored by on-going debates concerned with critical infrastructure security. Although not a comprehensive solution, one means of stimulating the inclusion of outer space assets in those debates may be to begin incorporating them within lists of critical infrastructures, such as the ones published by the US Department of Homeland Security (2012) and the Council of the European Union (2008a). There is the possibility that outer space infrastructures will be included within a future revision of the Council of the European Union’s critical infrastructure directive

(Anonymous, 2013), which may well act as the necessary stimulus. Indeed, there is evidence to suggest that the EU's position on European critical infrastructures is changing. The explicit inclusion of Galileo in a pilot programme concerned with inter- and intra-sector interdependencies (see European Commission, 2013b) arguably indicates a shift away from the narrow territorial boundaries which frame the existing ECI legislature.

As argued in chapter 3, although the Galileo and Copernicus programmes may not have been publically identified as being critical infrastructures, the impact they are expected to have with respect to other terrestrial critical infrastructures, and EU regional and external policies will arguably make them 'critical' upon completion. Once operational, Galileo will provide a series of navigation and positioning signals to users worldwide, enhancing services in the areas of aviation, Search and Rescue (SAR), land and maritime transportation and, last but not least, fishing. Although the majority of these services already benefit from signals transmitted by existing Global Navigation Satellite Systems (GNSSs) – in particular the US Global Positioning System (GPS) – Galileo will introduce further competition to the marketplace and is expected to offer improvements in terms of signal accuracy. Of note, the bi-directional SAR communication capabilities that Galileo will provide should be a significant enhancement of current capabilities. Moreover, the programme will extend European autonomy and independence in terms of its outer space capabilities; EU Member States and other states purchasing access will no longer be dependent solely upon GPS navigation and positioning signals, which the US reserves the right to deny. In terms of European space power therefore, Galileo can be considered a future critical outer space infrastructure both for the services it will provide and the independence it will ensure.

Like Galileo, Copernicus is not necessarily offering novel services and certainly not ones which are "essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions" (Council of the European Union, 2008a: L 345/77). However, it is expected to complement and enhance EU initiatives and policies in the areas of land, marine and atmospheric monitoring, emergency management and security. If successful, this policy-multiplication will make it a valuable resource to the EU and its Member States. Consequently, Copernicus can be considered to have the potential of being a critical outer space infrastructure through its expected contributions to European space power projection.

6.2 The security of European critical outer space infrastructures

Both the Galileo and Copernicus programmes have the potential to become critical outer space infrastructures once they are completed. As mentioned earlier though, outer space infrastructures are rarely included within debates over infrastructure security. With reference to the fourth question that this thesis has sought to answer, the EU's efforts to secure its critical outer space infrastructures have been conceptualised through the lens of anticipatory security.

The EU has two main strategies to enhance the security of the space segments of its critical outer space infrastructures: one at the diplomatic level, where it is attempting to assert leadership over outer space affairs – particularly in relation to preventing the weaponisation of outer space, the generation of space debris and the promotion of sustainability in outer space activities – and one at an internal level, where the EU and its Member States are actively developing technologies and programmes – such as the SSA and EU-led SST – to mitigate the environmental threats existing in near-Earth space and secure their satellites against the threats they cannot prevent. In addition to countering threats to European space assets, these aforementioned strategies reveal the EU's identification of specific risks and dangers as being threatening to the space segments of its critical outer space infrastructures. With reference to the third question that this thesis has sought to answer, these threats include intentional actions, such as the destruction of objects in outer space and unannounced manoeuvres resulting in collisions between space objects, and environmental hazards such as space debris and space weather phenomena.

By championing the draft Code of Conduct for Outer Space Activities, the EU is demonstrating its support for a non-legally binding initiative to promote 'good' practice by spacefaring actors. Whilst this good practice involves adhering to existing legal treaties, declarations and standards concerning outer space activities, the Code also represents a commitment by any who agree to it that they will avoid the intentional destruction of objects in outer space, with specific exceptions. As an anticipatory security mechanism, the Code is largely preemptive in its scope as well as containing some preventive elements. If the Code were to come to fruition, the recommended practices directed at the mitigation of further debris generation and orbital congestion are expected to contribute to long-term precautionary efforts to ensure sustainable outer space activities and avoid the onset of the Kessler Syndrome. Moreover, as well as seeking to restrict future debris generation, the Code is arguably attempting to reduce unexpected or unannounced manoeuvres of space objects through Transparency and Confidence-Building Measures (TCBMs), thus mitigating the element of surprise to other actors that such manoeuvres can introduce.

In terms of the environmental hazards discussed in chapter 5 as posing a danger to space segments of critical outer space infrastructures, there are two forms of preventive anticipatory mechanisms at play. The first is introducing resilience within outer space activities through the design of space objects and the inclusion of hardware redundancy, whilst the second is ensuring that operators can be forewarned of approaching space weather phenomena or impending collisions with space debris through SSA capabilities. Both these mechanisms are largely preventive in nature as they deal with imminent and existing risks and dangers, namely Space Weather Events (SWEs) and the extant space debris population. However, research into large-scale SWEs and the national and international space debris mitigation guidelines and standards offer an element of preemptive thinking by conditioning those working within their respective fields to the possibilities of future events, such as SWEs similar to the Carrington Event or the emergence of the Kessler Syndrome, at some orbital altitudes.

In addition to the mission-specific measures that can be introduced to enhance the resilience of individual satellites or programmes, the EU and its Member States continue to invest in Space Situational Awareness (SSA) capabilities. The European Parliament's approval of an EU-managed Space Surveillance and Tracking (SST) support framework in April 2014 is indicative of this continued investment and demonstrates the European desire to avoid being dependent upon the provision of data from the US Space Surveillance Network (USSSN), as well as concerns over the ageing technology at the heart of the USSSN (see European Commission, 2013a). As an anticipatory security mechanism, the three segments of the SSA –SST segment, the SWE segment and the Near-Earth Object (NEO) segment – are both preventive and preemptive in nature, although arguably more the former than the latter. Whilst there is an element of precaution, the ultimate objective of the SSA programme is to improve the statistical calculability of the threat(s) posed by environmental risks and dangers to both satellites and terrestrial societies, whilst simultaneously addressing the spatio-temporal uncertainties inherent within outer space security. The SST segment is arguably the most preventive of the three, as it acts solely upon the existing space debris population in order to catalogue and track debris in near-Earth space. The SWE segment does include research into both solar activity and the effects of SWEs upon satellites, making it both preemptive and preventive. Lastly, the NEO segment, although addressing a danger which does not pose a significant threat to satellites, is intended to search for NEOs with trajectories that may lead them on a collision course with the Earth. In this manner it is relatively precautionary in nature, however once if and when an NEO with such a trajectory is identified, the purpose of the NEO segment will be to calculate the probabilities of collision with the Earth, thus introducing an element of prevention.

The EU’s approach to outer space security is largely consistent with its terrestrial policies, reinforcing the argument that its outer space infrastructures are a means of policy-multiplication. Perhaps the most obvious example of the similarities between terrestrial and extra-terrestrial EU policies is the permeation of discourses on sustainability, which are a core feature of the Code and are also represented throughout projects associated with the Copernicus programme. That being said, the sustainability advocated through many EU policies is arguably not comprehensive. For instance, the EU-led SST programme does not mention SWEs or NEOs. Given that the Space Situational Awareness Preparatory Programme (SSA-PP) managed by ESA was a three-pronged approach to SSA, incorporating SST alongside the monitoring and tracking of SWEs and NEOs, questions are raised by the EU’s prioritisation of SST over SWEs and NEOs. On the one hand, the EC has argued that ESA lacks the competence to manage the highly confidential information an SST programme would require (European Commission, 2013a: 22), whilst SWE and NEO monitoring is already undertaken by civilian and scientific communities around the world. Nonetheless, it can be argued that the decision for the EU to manage only the SST segment of the SSA indicates a hierarchy of issues of concern for the security of outer space infrastructures, with space debris placed firmly above SWEs or NEOs. In other words, the EU appears to be anticipating that space debris will be a greater danger to its outer space infrastructures than SWEs or NEOs, hence its prioritisation.

Two forms of anticipatory security measures have been focused upon in this thesis; preventive actions are directed towards risks and dangers that are “statistically knowable and calculable according to cycles of regularity” (de Goede, 2011: 9), whilst preemptive measures are concerned with risks that are “irregular, incalculable, and, in important ways, unpredictable” (de Goede, 2011: 9). However, in the context of outer space anticipatory security varies slightly from its application to terrestrial affairs. As discussed in chapter 3, the inherent spatio-temporal uncertainties involved within outer space activities mean that even statistically calculable risks may pose unexpected danger to satellites. The notion of such ‘known’ risks being expected to run a “predictable, linear course from cause to effect” (Massumi, 2007: para. 5) is thus insufficient in terms of outer space security. Anticipatory security practices oriented towards outer space activities must therefore account not only for the generic danger posed by threats – the capacity for phenomena to cause damage to satellites and other space objects – but also the likelihood that specific satellites or other space objects will be exposed to those threats. Calculations of such a likelihood must take place on a regular, if not constant, basis, hence the need for situational awareness capabilities. Improving the situational awareness of near-Earth space is thus prominent within the majority of anticipatory security measures discussed in this thesis; as a situational awareness programme, the SSA is self-evident of this, however the importance of the commitment within the Code to informing other space actors of satellites’ manoeuvres must also be emphasised. Sustainable operations in outer space are dependent upon reducing the intrinsic spatio-temporal uncertainties, underlining de Montluc’s (2012) contention that “surveillance [conducted by SSA programmes] might in fact become a precondition of our capability to access space on acceptable security/safety terms and to conduct operational activities" (p. 199).

6.3 Opportunities for further research

During the research project from which this thesis stems, some themes and topics emerged which did not fit within the scope of the thesis, yet are deserving of further analysis. This section will outline these themes and topics, explaining why it is felt they are worthy of future research.

Beginning with the concept of space power, which has been discussed in some detail in chapters 1 and 2 of this thesis; there are three opportunities for further work to be done. Firstly, on how Galileo, Copernicus and, to some extent, the European SSA programmes, complement and contribute to European space power projection. The EC has voiced its belief that coordinated European space policies and strategies can "**enable it to exert global leadership in selected policy areas in accordance with European interests and values**" (European Commission, 2007b: 4, original emphasis), and, given the substantial financial and political investment into Galileo, Copernicus and other space programmes, it would appear that outer space is one of these policy areas. Moreover, the EU's championing of the Code indicates its desire for leadership in diplomatic matters concerned with outer space affairs. Although at the time of writing the future success of the Code is not assured, the document is arguably representative of the EU's efforts to impose its vision and values on other spacefaring actors, making it a tool of power projection. The criticality of Galileo and Copernicus has been partially assessed in thesis based upon their contributions to EU policy-multiplication and space power, but questions still exist on how these programmes, the Code and the planned SSA inform EU terrestrial policies and shape its space power projection.

Secondly, there is a need for further engagement with the astrographies and geographies of space power. With the exception of Dolman (1999; 2002) and France and Sellers (2011), little work has been done on the astrographical and astrophysical restrictions on space power capabilities. Moreover, the intrinsic relationship between space power and the conduct of terrestrial affairs deserves interrogation; particularly over whether the increasing academic attention to space power is blurring the boundary between the Earth and near-Earth space. There is a risk that near-Earth space – and mainly the orbital altitudes comprising LEO – will be normalised as an extension of the terrestrial military theatres of operations, harming efforts to maintain outer space as a domain free from deployed active weapons systems.

Lastly, the relationship between the concepts of space power and outer space security is also requiring further interrogation. For the purposes of this thesis these two concepts have been separated by their ultimate objectives; space power looks towards the enhancement of terrestrial policies and power, whilst outer space security is largely focused upon access to outer space and the conduct of operations within the domain. However, space power and outer space security are complementary and arguably mutually dependent. The former could not exist without the latter as it relies upon the provision of services from outer space infrastructures, whilst policy-multiplication and space power offer the justification for the continued development and deployment of outer space technologies and assets, without which debates over security in the domain would be redundant.

As stated in the introduction, this thesis has focused solely on the space segments of critical outer space infrastructures. Attention must also be paid to the ground segments in order to comprehensively assess the security of critical outer space infrastructures. Such a study will mostly likely include terrestrial environmental factors or political instability threatening the bilateral agreements between the host state and infrastructure owner. Moreover, given the argument of this thesis that the EU's approach to security of the space segments of its critical outer space infrastructures is based upon a logic of anticipatory security, the opportunity emerges to explore whether the security of ground segments is also anticipatory in nature.

Critical outer space infrastructures have been portrayed in this thesis as comprising of both physical and virtual elements. The materiality of the security is therefore problematized (see Aradau, 2010a), as there is a need to protect not only the hardware (the ground stations, launch facilities and satellites) but also the connectivity between the hardware. With respect to the ground stations, there is a need to incorporate issues surrounding their security into wider debates on outer space infrastructures. Jurisdictional and security matters concerning ground stations based on foreign territory from the operating state or actor have arguably not received the attention they deserve in academic debates in the discipline of International Relations. In addition, the combination of hardware and connectivity which comprise outer space infrastructures requires critical engagement with the materiality of outer space security. This has been discussed to some extent in this thesis with respect to frequency congestion and jamming and spoofing but there is nonetheless the need for further interrogation of whether the hardware underpins the connectivity, or vice versa. This in turn may impact discussions of the astrographies and geographies of outer space infrastructures; if it is argued that the connectivity in between satellites and/or between satellites and ground segments are more valuable than the outer space assets themselves, then it is possible that the focus of outer space security may shift towards the ground segments. Given that these segments are often located outside of the territorial borders of the operating actor or state, they may become perceived as points of vulnerability, hence the need mentioned earlier for their incorporation within debates over the security of outer space infrastructures.

Another area which emerged during this research project concerns imaginations and uses of near-Earth space. There is an opportunity for a ‘social construction of near-Earth space’ akin to P. E. Steinberg’s (2001) study of the Oceans, charting how the use of orbits has evolved and how dependence on technologies has changed since the launch of Sputnik. Moreover, the ‘real estate’ value of orbital space is beginning to extend beyond GEO/GSO, and the danger of the increasing space debris population, perhaps even leading to the Kessler Syndrome becoming a reality, has the potential to transform some orbital altitudes into no-go areas. This makes satellites in those regions both vulnerable and important given the possible future scarcity of secure orbital trajectories.

Finally, although this thesis has focused upon the conceptualisations of outer space security by the EU, the framework of anticipatory critical infrastructure security could be expanded to other actors with a high degree of dependence upon their outer space infrastructures, namely the US. Such a project might not only offer a variation on existing studies of US approaches to outer space security but would also be an opportunity to refine the framework through its application to a very different case study than the one used in this thesis.

Word Count: 83,491

References

Abulafia, D. (2008) *The Discovery of Mankind Atlantic Encounters in the Age of Columbus*, New Haven: Yale University Press.

Adey, P. (2010) *Aerial Life spaces, mobilities, affects*, Chichester: Wiley-Blackwell.

Adey, P. and B. Anderson (2012) 'Anticipating emergencies: Technologies of preparedness and the matter of security', *Security Dialogue*, 43(2): 99-117.

Agnew, J. (1994) 'The territorial trap: the geographical assumptions of international relations theory', *Review of International Political Economy*, 1(1): 53-80.

Agnew, J. (2005) 'Sovereignty Regimes: Territoriality and State Authority in Contemporary World Politics', *Annals of the Association of American Geographers*, 95(2): 437-461.

Agnew, J. (2010) 'Still Trapped in Territory?', *Geopolitics*, 15(4): 779-784.

Ailor, W. (2004) 'Collision Avoidance and Improving Space Surveillance', *Astropolitics*, 2(2): 107-120.

Ailor, W. H. (2006) 'Space traffic management: Implementations and implications', *Acta Astronautica*, 58(5): 279-286.

Ailor, W. H. and R. P. Patera (2007) 'Spacecraft re-entry strategies: meeting debris mitigation and ground safety requirements', *Proceedings of the Institution of Mechanical Engineers, Part G: Journal of Aerospace Engineering*, 221(6): 947-953.

Air Force Space Command Public Affairs (2012) 'AFSPC Milestone: First US ASAT intercept', *Air Force Space Command News*, [Online] http://www.afspc.af.mil/news/story.asp?id=123317577, Created: 15/09/12, Accessed: 25/09/12.

Aldridge, E. C. (1987) 'The myths of militarization of space', *International Security*, 11(4): 151-156.

Allianz Global Corporate & Speciality (2012) *Space Risks: A new generation of challenges*, Munich: Allianz Global Corporate & Speciality AG, [Online] https://www.allianz.com/v_1342876324000/media/press/document/agcs_space_risks_white_paper.pdf, Accessed: 16/08/13.

Amos, J. (2011) 'Europe's first Galileo satellites lift off', *BBC News Science & Environment*, [Online] http://www.bbc.co.uk/news/science-environment-15372540, Created: 21/10/11, Accessed: 19/03/12.

Amos, J. (2012a) 'Doubts hang over EU's Sentinel radar mission', *BBC News Science & Environment*, [Online] http://www.bbc.co.uk/news/science-environment-17050547, Created: 08/03/12, Accessed: 01/06/12.

Amos, J. (2012b) 'Envisat imaged by sharp-eyed Pleiades', *BBC News Science & Environment*, [Online] http://www.bbc.co.uk/news/science-environment-17790420, Created: 20/04/12, Accessed: 30/05/12.

Amos, J. (2012c) 'Grail gravity satellites slam into Moon', *BBC News Science & Environment*, [Online] http://www.bbc.co.uk/news/science-environment-20761903, Created: 17/12/12, Accessed: 16/08/13.

Amos, J. (2012d) 'UK design to "harpoon" old satellites', *BBC News Science & Environment*, [Online] http://www.bbc.co.uk/news/science-environment-19803461, Created: 02/10/12, Accessed: 21/01/13.

Anderson, B. (2010) 'Preemption, precaution, preparedness: Anticipatory action and future geographies', *Progress in Human Geography*, 34(6): 777-798.

Anselmo, L. and C. Pardini (2008) 'Space debris mitigation in geosynchronous orbit', *Advances in Space Research*, 41(7): 1091-1099.

Anonymous (2012a) 'Interview with a European Space Agency official', 26/03/12.

Anonymous (2012b) 'Interview with a European Space Agency official', 10/05/12.

Anonymous (2012c) 'Interview with a European Space Agency official', 31/07/12.

Anonymous (2012d) 'Interview with a United Kingdom Space Agency official', 10/08/12.

Anonymous (2012e) 'Interview with a European Space Agency official', 31/08/12.

Anonymous (2012f) 'Interview with a European Space Agency official', 19/09/12.

Anonymous (2013) 'Interview with a European Commission official', 25/02/13.

Aradau, C. (2010a) 'Security That Matters: Critical Infrastructure and Objects of Protection', *Security Dialogue*, 41(5): 491-514.

Aradau, C. (2010b) 'The myth of preparedness', *Radical Philosophy*, 161: 2-7.

Aradau, C. and R. Van Munster (2007) 'Governing Terrorism Through Risk: Taking Precautions, (un)Knowing the Future', *European Journal of International Relations*, 13(1): 89-115.

Aradau, C., L. Lobo-Guerrero and R. Van Munster (2008) 'Security, Technologies of Risk, and the Political: Guest Editors' Introduction', *Security Dialogue*, 39(2-3): 147-154.

Arbatov, A. and V. Dvorkin (eds.) (2010) *Outer Space Weapons, Diplomacy, and Security*, Washington D.C.: Carnegie Endowment for International Peace.

Arévalo-Yepes, C., A. Froelich, P. Martinez, N. Peter and K. Suzuki (2010) 'The Need for a United Nations space policy', *Space Policy*, 26 (1): 3-8.

Arianespace.com (2013) ‘Launcher family’, *Arianespace service & solutions – Launch Services*, [Online] http://www.arianespace.com/launch-services/launch-services-overview.asp, Accessed: 03/06/13.

Arianespace.com (2014) ‘Galileo satellites experience orbital injection anomaly on Soyuz launch: Initial report’, *Arianespace Press Release,* [Online] http://www.arianespace.com/news-press-release/2014/8-23-2014.asp, Created: 23/08/14, Accessed: 24/08/14.

Astrium (2011) ‘GMES’, *Astrium – Programmes,* [Online] http://www.astrium.eads.net/en/programme/gmes.html, Created: 14/11/11, Accessed: 02/06/12.

Babintsev, V. (2010) ‘The Peaceful and Military Development if Space: A Historical Perspective’ in: A. Arbatov and V. Dvorkin (eds.) *Outer Space Weapons, Diplomacy, and Security*, Washington D.C.: Carnegie Endowment for International Peace: 16-29.

Bailes, A. J. K. and I. Frommelt (eds.) (2004) *Business and Security: Public-Private Sector Relationships in a New Security Environment*, Oxford: Oxford University Press.

Baines, P. J. (2004) ‘Non-Offensive Defences: Space Protection Without Space-Based Weapons’, *Astropolitics*, 2(2): 149-174.

Banner, S. (2008) *Who Owns the Sky? The struggle to control airspace from the Wright brothers on*, Cambridge: MA: Harvard University Press.

Barroso, J. M. D. (2009) ‘The Ambitions of Europe in Space’, *Conference on European Space Policy Brussels, 15 October 2009*, SPEECH/09/476.

Baylis, J., K. Booth, J. Garnett and P. Williams (1975) *Contemporary Strategy*, London: Croom Helm.

Bell, D. and M. Parker (2009) *Space Travel and Culture*, Malden, MA: Blackwell Publishing.

Bell, J. (2005) *Doing your Research Project A guide for first-time researchers in education, health and social science*, Maidenhead: Open University Press.

Berenskoetter, F. (2007) ‘Thinking about power’ in: F. Berenskoetter and M. J. Williams (eds.) *Power in World Politics*, Abingdon: Routledge: 1-22.

Berenskoetter, F. and M. J. Williams (eds.) (2007) *Power in World Politics*, Abingdon: Routledge.

Bialasiewicz, L. (2008) ‘The Uncertain State(s) of Europe?’, *European Urban and Regional Studies*, 15(1): 71-82.

Black, G. (2011) *Satnav Dependence – The Reality*, [Online] http://www.google.co.uk/url?sa=t&rct=j&q=gordon%20black%2C%20logica&source=web&cd=6&ved=0CEIQFjAF&url=http%3A%2F%2Fconferences.theiet.org%2Fgnss%2F-

documents%2F005-black.cfm&ei=KWCeT_aWIorF8gPX3IiSDw&usg=AFQjCNHxokH8bQkqEioj6gcWuM6LzMGg6w, Accessed: 30/04/12.

Blanchard, W. F. (2003) ‘Achieving GPS-Galileo interoperability: the challenges ahead’, *Space Policy*, 19(2): 95-99.

Bolton, I. R. B. (2012), ‘Neo-realism and the Galileo and GPS negotiations’ in: N. Bormann and M. Sheehan (eds.) *Securing Outer Space*, Abingdon: Routledge: 186-204.

Bormann, N. (2012) ‘The lost dimension? A spatial reading of US weaponisation in space’ in: N. Bormann and M. Sheehan (eds.) *Securing Outer Space*, Abingdon: Routledge: 76-90.

Bormann, N. and M. Sheehan (eds.) (2012) *Securing Outer Space*, Abingdon: Routledge.

Brachet, G. (2012) ‘The origins of the “Long-term Sustainability of Outer Space Activities” initiative at UN COPUOS”, *Space Policy*, 28(3): 161-165.

Brunner, E. and M. Suter (2009) *International CIIP Handbook 2008/2009 An Inventory of 25 National and 7 International Critical Information Infrastructure Protection Policies*, Zurich: Centre for Security Studies, ETH Zurich.

Bryman, A. (2008) *Social Research Methods*, Third Edition, Oxford: Oxford University Press.

Budd, L. and P. Adey (2009) ‘The software-simulated airworld: anticipatory code and affective aeromobilities’, *Environment and Planning A*, 41(6): 1366-1385.

Burgess, J. P. (2007) ‘Social values and material threat: the European Programme for Critical Infrastructure Protection’, *International Journal of Critical Infrastructures*, 3(3-4): 471-487.

Butler, A. (2011) ‘Lights Out fort the Airborne Laser’, *Aviation Week*, [Online] http://www.aviationweek.com/Article.aspx?id=/article-xml/asd_12_21_2011_p01-02-408678.xml&p=1, Created: 21/12/11, Accessed: 04/10/12.

Butler, D. L. (2001) ‘Technogeopolitics and the struggle for control of world air routes’, *Political Geography*, 20(5): 635-658.

Cadbury, D. (2005) *Space Race The Untold Story of Two Rivals & Their Struggle For the Moon*, London: Fourth State.

Caldicott, H. and C. Eisendrath (2007) *War in Heaven the arms race in outer space*, New York: The New Press.

Cameron, A. (2014) ‘GLONASS Gone … Then Back’, *GPS World*, [Online] http://gpsworld.com/glonass-gone-then-back/, Created: 02/04/14, Accessed: 18/06/14.

Campbell, D. (1998) *Writing Security United States Foreign Policy and the Politics of Identity*, Manchester: Manchester University.

Campbell, J. and R. H. Wynne (2011) *Introduction to Remote Sensing*, Fifth Edition, New York: The Guildford Press.

Carter, S. and D. P. McCormack (2010) 'Affectivity and Geopolitical Images' in: F. MacDonald, R. Hughes and K. Dodds (eds.) *Observing States Geopolitics and Visual Culture*, I. B. Tauris & Co. Ltd.: 104-122.

Castells, M. (2001) *The Internet Galaxy Reflections on the Internet, Business, and Society*, Oxford: Oxford University Press.

Centre National D'Études Spatiales (2009) 'Are there solutions?', *Debris-spatiaux.cnes.fr*, [Online] http://debris-spatiaux.cnes.fr/english/existe_solution_eng.html, Created: 27/02/09, Accessed: 12/02/13.

Centre National D'Études Spatiales (2012) 'Pleiades: a multi-missions concept and a partnership program', *PLEIADES Dual optical system for metric resolution observations*, [Online] http://smsc.cnes.fr/PLEIADES/, Created: 05/01/12, Accessed: 22/05/12.

Christian, E. L. (2003) *Meteoroid/Debris Shielding*, TP-2003-210788, Houston, TX: National Aeronautics and Space Administration, [Online] http://ston.jsc.nasa.gov/collections/TRS/_techrep/TP-2003-210788.pdf, Created: 03/10/03, Accessed: 12/02/13.

Christian, E. R. and A. J. Davis (2012) 'Advanced Composition Explorer (ACE) Mission Overview', *Advanced Composition Explorer*, [Online] http://www.srl.caltech.edu/ACE/ace_mission.html, Created: 27/01/12, Accessed: 17/09/12.

Clark, S. (2014) 'European navigation craft launched into wrong orbit', *Spaceflightnow.com* [Online] http://spaceflightnow.com/soyuz/vs09/140822anomaly/, Created: 22/08/14, Accessed: 23/08/14.

Clemente, D. (2013) *Cyber Security and Global Interdependence: What is Critical?*, London: Chatham House.

Clinton, W. J. (1996) *Executive Order 13010 – Critical Infrastructure Protection*, 15/07/1996, [Online] http://www.presidency.ucsb.edu/ws/?pid=53066, Accessed: 29/10/12.

Cock, J. (1989) 'Keeping the fires burning: militarisation and the politics of gender in South Africa', *Review of African Political Economy*, 16(4-5): 50-64.

Close, S., M. C. Kelley, A. Fletcher, N. Lee and P. Colestock (2011) 'RF Signatures of Hypervelocity Impacts on Spacecraft', *3rd AIAA Atmospheric Space Environments Conference 27-30 June 2011*, [Online] http://sess.stanford.edu/sites/default/files/pubs/conf/201106%20-%20AIAA%20ASE%20-%20RF%20signatures.pdf, Created: 29/06/11, Accessed: 23/07/13.

Cohen, F. (2010) ‘What makes critical infrastructures *Critical*?’, *International Journal of Critical Infrastructure Protection*, 3(2): 53-54.

Collis, C. (2009) ‘The geostationary orbit: a critical legal geography of space’s most valuable real estate’ in: D. Bell and M. Parker (eds.) *Space Travel and Culture*, Malden, MA: Blackwell Publishing: 47-65.

Committee on the Societal and Economic Impacts of Severe Space Weather Events: A Workshop (2008) Severe Space Weather Events - Understanding Societal and Economic Impacts A Workshop Report. Washington, D.C.: The National Academies Press.

Conference on Disarmament (2008) *Letter dated 12 February 2008 from the Permanent Representative of the Russian Federation and the Permanent Representative of China to the Conference on Disarmament addressed to the Secretary-General of the Conference transmitting the Russian and Chinese texts of the Draft “Treaty on Prevention of the Placement of Weapons in Outer Space and of the Threat or Use of Force Against Outer Space Objects (PPWT)” introduced by the Russian Federation and China*, CD/1839.

Consultative Committee for Space Data Systems (2006a) *Security Threats Against Space Missions*, CCSDS 350.1-G-1, Washington, D.C.: CCSDS Secretariat.

Consultative Committee for Space Data Systems (2006b) *The Application of CCSDS Protocols to Secure Systems*, CCSDS 350.0-G-2, Washington, D.C.: CCSDS Secretariat.

Consultative Committee for Space Data Systems (2012) *Security Architecture For Space Data Systems*, CCSDS 351.0-M-1, Washington, D.C.: CCSDS Secretariat.

Consultative Committee for Space Data Systems (2013a) ‘About CCSDS’, *CCSDS.org – About*, [Online] http://public.ccsds.org/about/default.aspx, Accessed: 16/08/13.

Consultative Committee for Space Data Systems (2013b) ‘Member Agencies’, *CCSDS.org – Participation*, [Online] http://public.ccsds.org/participation/member_agencies.aspx, Accessed: 16/08/13.

Cooper, L. (2003) ‘The Strategy of Responsive Space’, *Astropolitics*, 1(3): 44-62.

Copernicus.eu (2013a) ‘Database of projects – IncREO’, *Copernicus The European Earth Observation Programme*, [Online] http://copernicus.eu/pages-principales/projects/project-database/database-of-projects/?idproj=275&what=1&filter=9&page=0&cHash=32d1edf6eaf71079727a3d89b95f97b2, Accessed: 15/03/13.

Copernicus.eu (2013b) ‘Emergency Management’, *Copernicus The European Earth Observation Programme*, [Online] http://copernicus.eu/pages-principales/projects/other-fp7-projects/emergency-management/, Accessed: 15/03/13.

Copernicus.eu (2013c) ‘Priority Areas for Security Applications (Draft for validation by EC)’, *Copernicus The European Earth Observation Programme*, [Online] http://copernicus.eu/pages-principales/services/security-draft-for-validation-by-ec/priority-areas-for-security-applications-draft-for-validation-by-ec/, Accessed: 20/03/13.

Copernicus.eu (2013d) 'Services', *Copernicus The European Earth Observation Programme*, [Online] http://copernicus.eu/pages-principales/services/, Accessed: 13/03/13.

Council of the European Union (2000) 'Council Resolution of 16 November 2000 on a European Space Strategy', *Official Journal of the European Communities*, 23/12/00: C 371/2-C 371/3.

Council of the European Union (2007) *Resolution on the European Space Policy*, 10037/07 ANNEX, Brussels: Council of the European Union.

Council of the European Union (2008a) 'Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection', *Official Journal of the European Union*, 23/12/2008: L 345/75-L 345/82.

Council of the European Union (2008b) *Council Conclusions and draft Code of Conduct for outer space activities*, 17175/08, Brussels: Council of the European Union.

Council of the European Union (2010) *Council Resolution: 'Global Challenges: taking full benefit of European space systems'*, 16865/10, Brussels: Council of the European Union.

Council of the European Union (2011) 'Council Resolution of 6 December 2011 'Orientations concerning added value and benefits of space for the security of European citizens', *Official Journal of the European Union*, 23/12/11, C 377/1-C 377/4.

Council of the European Union (2012) 'Council Decision 2012/281/CFSP of 29 May 2012 in the framework of the European Security Strategy in support of the Union proposal for an international Code of Conduct on outer-space activities', *Official Journal of the European Union*, 30/05/12: L 140/68-L 149/73.

Council of the European Union (2013) 'Council Decision of 3 December 2013 establishing the specific programme implementing Horizon 2020 – the Framework Programme for Research and Innovation (2014-2020) and repealing Decisions 2006/971/EC, 2006/972/EC, 2006/973/EC, 2006/974/EC and 2006/975/EC', *Official Journal of the European Union*, 20/12/13: L 347/965-L 347/1041.

Coward, M. (2009) 'Network-Centric Violence, Critical Infrastructure and the Urbanization of Security', *Security Dialogue*, 40(4-5): 399-418.

Crampton, J. W. and S. Elden (eds.) (2009) *Space, Knowledge and Power Foucault and Geography*, Farnham: Ashgate Publishing Limited.

Crowther, R. (2002) 'Space Junk: Protecting Space for Future Generations', *Science*, 296(5571): 1241-1242.

Crowther, R. (2003) 'Orbital Debris: A Growing Threat to Space Operations', *Philosophical Transactions: Mathematical, Physical and Engineering Sciences*, 361: 157-168.

Cukurtepe, H. and I. Akgun (2009) 'Towards space traffic management system', *Acta Astronautica*, 65(5-6): 870-878.

Dalby, S. (2008) 'Imperialism, Domination, Culture: The Continued Relevance of Critical Geopolitics', *Geopolitics*, 13(3): 413-436.

Dalby, S. (2010) 'Recontextualising violence, power and nature: The next twenty years of critical geopolitics?', *Political Geography*, 29(5): 280-288.

Dant, D. (2010) 'Addressing Opportunities and Challenges of the Strategic Environment', *Astropolitics*, 8(2-3): 170-174.

de Goede, M. (2008a) 'Beyond Risk: Premediation and the Post-9/11 Security Imagination', *Security Dialogue*, 39(2-3): 155-176.

de Goede, M. (2008b) 'The Politics of Preemption and the War on Terror in Europe', *European Journal of International Relations*, 14(1): 161-185.

de Goede, M. (2011) *European Security Culture Preemption and Precaution in European Security*, Amsterdam: Vossiuspers UvA.

de Goede, M. and S. Randalls (2009) 'Precaution, pre-emption: arts and technologies of the actionable future', *Environment and Planning D: Society and Space*, 27(5): 859-878.

de Montluc, B. (2012) 'SSA: Where does Europe stand now?', *Space Policy*, 28(3): 199-201.

de Selding, P. B. (2010) 'European Officials Poised To Remove Chinese Payloads From Galileo Sats', *Space News – Civil Space*, [Online] http://www.spacenews.com/article/european-officials-poised-remove-chinese-payloads-galileo-sats, Created: 12/03/13, Accessed: 13/08/13.

de Selding, P. B. (2011a) 'European GMES Program at Risk as Battle Over Funding Escalates', *Space News – Civil*, [Online] http://www.spacenews.com/civil/111110-budget-battle-threatens-gmes.html, Created: 10/11/11, Accessed: 02/06/12.

de Selding, P. B. (2011b) 'New pressure to add GMES back to long-term budget', *Space News – Civil*, [Online] http://www.spacenews.com/civil/111411-european-commission-pressured-add-gmes-back-long-term-budget.html, Created: 14/11/11, Accessed: 01/06/12.

de Selding, P. B. (2012a) 'Envisat Failure Changes ESA Calculus on Sentinel Launches', *Space News – Policy*, [Online] http://spacenews.com/policy/120606-envisat-failure-sentinel-launches.html, Created: 06/06/12, Accessed: 07/06/12.

de Selding, P. B. (2012b) 'ESA, European Commission Near GMES Funding Rubicon', *Space News – Civil*, [Online] http://www.spacenews.com/civil/200220-esa-european-commission-near-gmes-funding-rubicon.html, Created: 20/02/12, Accessed: 02/06/12.

de Selding, P. B. (2012c) ‘European Union Defers GMES Funding Decision’, *Space News – Policy*, [Online] http://www.spacenews.com/policy/120529-eu-defers-gmes-funding-decision.html, Created: 29/05/12, Accessed: 02/06/12.

de Selding, P. B. (2013) ‘Europe Urged to Halt Work on ‘Dead End’ Ariane 6 Design’, *Space News – Launch Report*, [Online] http://www.spacenews.com/article/launch-report/35546europe-urged-to-halt-work-on-%E2%80%98dead-end-ariane-6-design#.UayWtEDI3ng, Created: 30/05/13, Accessed: 03/06/13.

DeBlois, B. M. (ed.) (1999) *Beyond the Paths of Heaven The Emergence of Space Power Thought*, Maxwell Air Force Base, AL: Air University Press.

Denemark, R. A. (ed.) (2010) *The International Studies Encyclopedia*, Wiley-Blackwell Publishing, Blackwell Reference Online 2010.

Denzin, N. K. and Y. S. Lincoln (eds.) (2003) *Collecting and Interpreting Qualitative Materials*, Thousand Oaks: Sage Publications.

Der Derian, J. (ed.) (2009a) *Critical Practices in International Theory Selected Essays*, Abingdon: Routledge.

Der Derian, J. (2009b) ‘Cyberwar, videogames and the Gulf War syndrome’ in: J. Der Derian (ed.) *Critical Practices in International Theory Selected Essays*, Abingdon: Routledge: 120-136.

Deudney, D. (1985) ‘Forging Missiles into Spaceships’, *World Policy Journal*, 2(2): 271-303.

Diez, T. (2006) ‘The Paradoxes of Europe’s Borders’, *Comparative European Politics*, 4(2/3): 235-252.

Dodds, K. (2008) ‘Icy Geopolitics’, *Environment and Planning D: Society and Space*, 26(1): 1-6.

Dodds, K. (2010a) ‘Classical Geopolitics Revisited’ in: R. A. Denemark (ed.) *The International Studies Encyclopedia*, Wiley-Blackwell Publishing, Blackwell Reference Online 2010, [Online], http://www.isacompendium.com/subscriber/tocnode?id=g9781444336597_chunk_g9781443365975_ss1-8, Accessed: 26/03/10.

Dodds, K. (2010b) ‘Flag planting and finger pointing: The Law of the Sea, the Arctic and the political geographies of outer continental shelf’, *Political Geography*, 29(2): 63-73.

Dolman, E. C. (1999) 'Geostrategy in the Space Age: An Astropolitical Analysis' in: C. S. Gray and G. Sloan (eds.), *Geopolitics Geography and Strategy*, London: Frank Cass: 83-106.

Dolman, E. C. (2002) *Astropolitik Classical Geopolitics in the Space Age*, Abingdon: Frank Cass.

Dolman, E. C. (2006) 'A Debate About Weapons in Space: For U.S. Military Transformation and Weapons in Space', *SAIS Review*, 26(1): 163-175.

Dolman, E. C. (2010) 'The Case for Weapons in Space: A Geopolitical Assessment', *APSA Annual Meeting* [Online] http://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID1678002_code1532576.pdf?abstractid=1676919&mirid=1, Created: 17/09/10, Accessed: 19/08/13.

Dolman, E. C. and H. F. Cooper Jr. (2011) 'Increasing the Military Uses of Space', [Online] http://www.ndu.edu/press/lib/pdf/spacepower/space-Ch19.pdf, Created: 06/06/11, Accessed: 19/07/13.

Duffy, B. (2005) 'The analysis of documentary evidence' in: J. Bell, *Doing your Research Project A guide for first-time researchers in education, health and social science*, Maidenhead: Open University Press: 122-135.

Dunn, M. (2006) 'Understanding Critical Information Infrastructures: An Elusive Quest' in: M. Dunn and V. Mauer (eds.) *International CIIP Handbook 2006 Vol. II Analyzing Issues, Challenges, and Prospects*, Zurich: Centre for Security Studies, ETH Zurich: 27-53.

Dunn, M. and V. Mauer (eds.) (2006) *International CIIP Handbook 2006 Vol. II Analyzing Issues, Challenges, and Prospects*, Zurich: Centre for Security Studies, ETH Zurich.

Dunn Cavelty, M. (2008) *Cyber-Security and Threats US efforts to secure the information age*, Abingdon: Routledge.

Duvall, R. and J. Havercroft (2008) 'Taking Sovereignty Out of this World: Space Weapons and Empire of the Future', *Review of International Studies*, 34(4): 755-775.

Dvorkin, V. (2010) 'Space Weapons Programs' in: A. Arbatov and V. Dvorkin (eds.) *Outer Space Weapons, Diplomacy, and Security*, Washington D.C.: Carnegie Endowment for International Peace: 31-45.

Egan, M. J. (2007) 'Anticipating Future Vulnerability: Defining Characteristics of Increasingly Critical Infrastructure-like Systems', *Journal of Contingencies and Crisis Management*, 15(1): 4-17.

Elden, S. (2010) 'Thinking Territory Historically', *Geopolitics*, 15(4): 757-761.

Elhefnawy, N. (2003) 'Territorializing space? Revising an old idea', *Astropolitics*, 1(2): 55-63.

Eurocontrol (2010a) 'Implementing Approaches with Vertical Guidance Using EGNOS', [Online] http://www.eurocontrol.int/eec/public/standard_page/ETN_2010_2_APV.html, Created: 01/07/2010, Accessed: 02/12/10.

Eurocontrol (2010b) 'Satellite Based Augmentation Systems', *Eurocontrol Navigation Domain*, [Online] http://www.ecacnav.com/RNAV_Applications/SBAS, Accessed: 08/01/11.

Europa.eu (2006) ‘Satellite Navigation: Galileo’, *Europa Summaries of EU legislation*, [Online] http://europa.eu/legislation_summaries/internal_market/single_market_for_goods/motor_vehicles/interactions_industry_policies/l24205_en.htm, Created: 13/01/06, Accessed: 19/03/12.

Europa.eu (2013) ‘Context: the European Year of Citizens 2013’, *European Year of Citizens 2013*, [Online] http://europa.eu/citizens-2013/en/about/context, Created: 13/05/13, Accessed: 10/06/13.

European Commission (1999) *Communication from the Commission Galileo Involving Europe in a New Generation of Satellite Navigation Services*, COM(1999) 54 final, Brussels: Commission of the European Communities.

European Commission (2000a) *Commission Communication to the European Parliament and the Council on GALILEO*, COM(2000) 750 final, Brussels: Commission of the European Communities.

European Commission (2000b) *Communication from the Commission on the precautionary principle*, COM(2000) 1, Brussels: Commission of the European Communities.

European Commission (2004) *Communication from the Commission to the Council and the European Parliament Critical Infrastructure Protection in the fight against terrorism*, COM(2004) 702 final, Brussels: Commission of the European Communities.

European Commission (2005) *Communication from the Commission to the Council and the European Parliament Global Monitoring for Environment and Security (GMES): From Concept to Reality*, COM(2005) 565 final, Brussels: Commission of the European Communities.

European Commission (2006a) *Communication from the Commission on a European Programme for Critical Infrastructure Protection*, COM(2006) 786 final, Brussels: Commission of the European Communities.

European Commission (2006b) *Green Paper on Satellite Navigation Applications*, COM(2006) 769 Final/2, Brussels: Commission for the European Communities.

European Commission (2007a) *Communication from the Commission State of progress with the project to implement the new generation European air traffic management system (SESAR)*, COM(2007) 103 final, Brussels: Commission of the European Communities.

European Commission (2007b) *Communication from the Commission to the Council and European Parliament European Space Policy*, COM(2007) 212 Final, Brussels: Commission of the European Communities.

European Commission (2007c) *Communication from the Commission to the European Parliament and the Council Progressing Galileo: Re-profiling the European GNSS*

Programmes, COM(2007) 534 Final, Brussels: Commission of the European Communities.

European Commission (2008) *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Global Monitoring for Environment and Security (GMES): we care for a safer planet*, COM(2008) 748 Final, Brussels: Commission of the European Communities.

European Commission (2009) *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Global Monitoring for Environment and Security (GMES): Challenges and Next Steps for the Space Component*, COM(2009) 589 Final, Brussels, Commission of the European Communities.

European Commission (2010) *Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions Action Plan on Global Navigation Satellite System (GNSS) Applications*, COM(2010) 308 final, Brussels: European Commission.

European Commission (2011a) *Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions towards a space strategy for the European Union that benefits its citizens*, COM(2011) 152 Final, Brussels: European Commission.

European Commission (2011b) *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions A Budget for Europe 2020*, COM(2011) 500 final, Brussels: European Commission.

European Commission (2012a) ‘Commission Implementing Decision of 23 February 2012 establishing a list of key decision points to evaluate the implementation of the Galileo programme with regard to the ground-based centres and stations to be created as part of the programme development and deployment (2012/117/EU)’, *Official Journal of the European Union*, 24/02/12: L 52/28-L 52/31.

European Commission (2012b) *Communication from the Commission to the Council and the European Parliament Establishing appropriate relations between the EU and the European Space Agency*, COM(2012) 617, Brussels: European Commission.

European Commission (2012c) *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the establishment of an Intergovernmental Agreement for the operations of the European Earth monitoring programme (GMES) from 2014-2020*, COM(2012) 218 final, Brussels: European Commission.

European Commission (2013a) *Commission Staff Working Document Impact Assessment* Accompanying the document *Proposal for a Decision of the European Parliament and of the Council establishing a space surveillance and tracking support programme*, SWD(2013) 55 final, Brussels: European Commission.

European Commission (2013b) *Commission Staff Working Document on a new approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures more secure*, SWD(2013) 318 final. Brussels: European Commission.

European Commission (2013c) *Memo Avoiding damage from space debris – space surveillance and tracking proposal*, [Online] http://europa.eu/rapid/press-release_MEMO-13-149_en.htm, Created: 28/02/13, Accessed: 24/04/13.

European Commission (2013d) *Proposal for a Decision of the European Parliament and of the Council Establishing a space surveillance and tracking support programme*, COM(2013) 107 final, Brussels: European Commission.

European Commission and European Space Agency (2010) *EC/ESA Joint Secretariat Paper Space and Security*, [Online] http://www.europarl.europa.eu/meetdocs/2009_2014/documents/sede/dv/sede170310ecesaspaceandsecurity_/sede170310ecesaspaceandsecurity_en.pdf, Created: 15/03/10, Accessed: 04/07/11.

European Commission Directorate-General for Energy and Transport (2009) *EGNOS Service Definition Document Open Service*, EGN-SDD OS V1.1, [Online] http://egnos-portal.gsa.europa.eu/sites/default/files/content/documents/egnos-service-definition_en.pdf, Created: 30/10/09, Accessed: 19/04/12.

European Commission Directorate-General for Enterprise and Industry (2011) *EGNOS Safety of Life Service Definition Document*, EGN-SDD SoL, V1.0, [Online] http://ec.europa.eu/enterprise/policies/satnav/egnos/files/egnos-sol-sdd-v1.0_en.pdf, Created: 17/02/11, Accessed: 13/12/12.

European Commission Enterprise and Industry (2013) 'Galileo – What do we want to achieve?', *Satellite Navigation – Galileo*, [Online] http://ec.europa.eu/enterprise/policies/satnav/galileo/index_en.htm#h2-7, Created: 14/03/13, Accessed: 18/08/13.

European Commission Mobility and Transport (2012) 'Intelligent Transport Systems – Road', *European Commission Mobility and Transport – Transport Themes*, [Online] http://ec.europa.eu/transport/themes/its/road/index_en.htm, Created: 09/10/12, Accessed: 19/12/12.

European Council (2013) *Conclusions (Multiannual Financial Framework)*, EUCO 37/13, Brussels: European Council.

European Defence Agency (2011) 'MUSIS', *European Defence Agency*, [Online] http://eda.europa.eu/Capabilitiespriorities/coredrivers/Space/Earthobservation/MUSIS, Accessed: 22/05/12.

European GNSS Supervisory Authority (2009) *EGNOS: making landing approaches more precise and efficient*, [Online] https://knowledge.gsa.europa.eu/livelink/livelink.exe/447556/2009-12-15_EGNOS_-

_Making_Landing_Approaches_More_Precise_and_Efficient.pdf?func=doc.Fetch&nodeid=447556&vernum=2, Created: 15/12/09, Accessed: 23/04/12.

European Space Agency (2005) ‘Closer Ties Between ESA and Russia’, *Esa.int Industry Portal* [Online] http://www.esa.int/About_Us/Industry/Industry_how_to_do_business/Closer_ties_between_ESA_and_Russia, Created: 19/01/05, Accessed: 03/06/13.

European Space Agency (2007) *Full deployment and operations Galileo System*, [Online] http://www.esa.int/esaNA/SEM5K8W797E_galileo_2.html, Created: 16/08/07, Accessed: 07/09/11.

European Space Agency (2011) ‘What is Galileo?’, *ESA The Future – Galileo*, [Online] http://www.esa.int/Our_Activities/Navigation/The_future_-_Galileo/What_is_Galileo, Created: 21/10/11, Accessed: 18/12/12.

European Space Agency (2012a) ‘ESA declares end of mission for Envisat’, *ESA News*, [Online] http://www.esa.int/esaCP/SEM1SXSWT1H_index_0.html, Created: 09/05/12, Accessed: 31/05/12.

European Space Agency (2012b) ‘ESA’s Sentinel Satellites’, *ESA GMES observing the earth*, [Online] http://www.esa.int/esaLP/SEM097EH1TF_LPgmes_0.html, Created: 16/03/12, Accessed: 22/05/12.

European Space Agency (2012c) ‘History’, *ESA Earthnet Online*, [Online] https://earth.esa.int/web/guest/missions/esa-operational-eo-missions/envisat/history, Accessed: 30/05/12.

European Space Agency (2012d) *Sentinel-1 ESA's Radar Observatory Mission for GMES Operational Services*, SP-1322/1, Noordwijk: ESA Communications.

European Space Agency (2012e) *Sentinel-2 ESA's Optical High Resolution Mission for GMES Operational Services*, SP-1322/2, Noordwijk: ESA Communications.

European Space Agency (2012f) *Sentinel-3 ESA's Global Land and Ocean Mission for GMES Operational Services*, SP-1322/3, Noordwijk: ESA Communications.

European Space Agency (2012g) ‘What is EGNOS?’, *ESA Egnos Navigation*, [Online] http://www.esa.int/esaNA/egnos.html, Created: 12/02/12, Accessed: 19/04/12.

European Space Agency (2013a) ‘Ariane 6’, *ESA – Launch Vehicles*, [Online] http://www.esa.int/Our_Activities/Launchers/Launch_vehicles/Ariane_6, Created: 18/04/13, Accessed: 03/06/13.

European Space Agency (2013b) ‘Clean Space’, *ESA – clean space*, [Online] http://www.esa.int/TEC/Clean_Space/, Created: 10/04/13, Accessed: 15/07/13.

European Space Agency (2013c) ‘Galileo fixes Europe’s position in history’, *ESA Navigation*, [Online] http://www.esa.int/Our_Activities/Navigation/Galileo_fixes_Europe_s_position_in_history, Created: 12/03/13, Accessed: 22/03/1

European Space Agency (2013d) 'Near-Earth Objects – NEO Segment', *ESA – Space Situational Awareness*, [Online] http://www.esa.int/Our_Activities/Operations/Space_Situational_Awareness/Near-Earth_Objects_-_NEO_Segment, Accessed: 19/06/13.

European Space Agency (2013e) *Sentinel-2 The Operational Copernicus Optical High Resolution Land Mission*, [Online] http://esamultimedia.esa.int/docs/S2-Data_Sheet.pdf, Accessed: 18/06/14.

European Space Agency (2013f) *Sentine-3 Copernicus Medium Resolution Land and Ocean Mission*, [Online] http://esamultimedia.esa.int/docs/S3-Data_Sheet.pdf, Accessed: 18/06/14.

European Space Agency (2014a) 'Sentinel-1', *ESA Future Missions – Copernicus – Sentinels*, [Online] https://earth.esa.int/web/guest/missions/esa-future-missions/sentinel-1, Accessed: 18/06/14.

European Space Agency (2014b) 'Sentinel-1', *ESA – Our Activities – Observing the Earth*, [Online] http://www.esa.int/Our_Activities/Observing_the_Earth/Copernicus/Sentinel-1/Facts_and_figures, Accessed: 08/05/14.

European Space Agency (2014c) 'Sentinel-2', *ESA – Our Activities – Observing the Earth*, [Online] http://www.esa.int/Our_Activities/Observing_the_Earth/Copernicus/Sentinel-2, Accessed: 08/05/14.

European Space Agency (2014d) 'Sentinel-3', *ESA – Our Activities – Observing the Earth*, [Online] http://www.esa.int/Our_Activities/Observing_the_Earth/Copernicus/Sentinel-3, Accessed: 08/05/14.

European Space Agency (2014e) 'Sentinels-4/-5 and -5P', *ESA – Our Activities – Observing the Earth*, [Online] http://www.esa.int/Our_Activities/Observing_the_Earth/Copernicus/Sentinels_-4_-5_and_-5P, Accessed: 08/05/14.

European Space Agency Director General (2003) *Agenda 2007 – A Document by the ESA Director General*, BR-213, Noordwijk: ESA Publications Division.

European Space Agency Director General's Office (2008) *Space Debris Mitigation for Agency Projects*, ESA/ADMIN/IPOL(2008)2, [Online] http://www.cnsa.gov.cn/n615708/n676979/n676983/n893604/appendix/200852915833.pdf, Created: 26/05/2008, Accessed: 03/08/2012.

European Space Agency Ministerial Council (2012) *Resolution on the role of ESA in sustaining competitiveness and growth in Europe*, ESA/C-M/CCXXXIV/Res. 1, [Online] http://esamultimedia.esa.int/docs/MinisterialCouncil/ESA-C-2012-186.pdf, Created: 01/02/13, Accessed: 27/03/13.

European Union (2013) *Draft International Code of Conduct for Outer Space Activities*, Available at: http://eeas.europa.eu/non-proliferation-and-disarmament/pdf/space_code_conduct_draft_vers_16_sept_2013_en.pdf (accessed 2 December 2013).

European Union (2014) 'DECISION OF THE EUROPEAN PARLIAMENT OF THE COUNCIL establishing a Framework for Space Surveillance and Tracking support', 2013/0064 (COD).

Firth, S. (2013) 'Stanford scientist closes in on a mystery that impedes space exploration', *Stanford – News*, [Online] http://news.stanford.edu/news/2013/february/space-dust-threat-022613.html, Created: 26/02/13, Accessed: 23/07/13.

Flynn, N. (1986) *War in Space*, Leicester: Windward.

Foucault, M. (2009) 'Meshes of Power', translated by G. Moore in: J. W. Crampton and S. Elden (eds.) *Space, Knowledge and Power Foucault and Geography*, Farnham: Ashgate Publishing Limited: 153-162.

Foust, J. (2012) 'Key space issues for 2013', *The Space Review essays and commentaries about the final frontier*, [Online] http://thespacereview.com/article/2211/1, Created: 31/12/12, Accessed: 07/01/13.

France, M. E. and J. J. Sellers (2011) 'Real Constraints on Spacepower', [Online] http://www.ndu.edu/press/lib/pdf/spacepower/space-Ch4.pdf, Created: 06/06/11, Accessed: 20/06/13.

Fuller Jr., J., J. Foust, C. Frappier, D. Kaiser and D. Vaccaro (2011) 'The Commercial Space Industry: A Critical Spacepower Consideration', [Online] http://www.ndu.edu/press/lib/pdf/spacepower/space-Ch6.pdf, Created: 06/06/11, Accessed: 16/06/13.

Galileo Joint Undertaking (2005) *GALILEO Research and Development Activities Call 8608 Galileo Time and Synchronization Applications Statement of Work*, [Online] http://www.gsa.europa.eu/sites/default/files/content/8068_en.pdf, Created: 07/12/05, Accessed: 22/03/13.

Ganushkina, N. Y., I. Dandouras, Y. Y. Shprits and J. Cao (2011) 'Locations of boundaries of outer and inner belts as observed by Cluster and Double Star', *Journal of Geophysical Research*, 116: 1-18.

Garbin, D. A. and J. F. Shortle (2007) 'Measuring Resilience in Network-Based Infrastructures' in: J. A. McCarthy, C. Pommerening, L. J. Perelman, P. L. Scalingi, D. A. Garbin, J. F. Shortle, D. Arsenault, A. Sood, D. B. Moody, E. M. Jackson, *Critical Thinking: Moving from Infrastructure Protection to Infrastructure Resilience*, George Mason University CIP Program Discussion Paper Series: 73-86.

Garnett, J. (1975) 'The Role of Military Power' in: J. Baylis, K. Booth, J. Garnett and P. Williams, *Contemporary Strategy*, London: Croom Helm: 50-64.

Gattolin, A. (2013) *Proposition de Résolution Europééne Présentée au nom de la Commission des Affaires Européennes en application de l'Article 73* Quater *du Règlement sur la* ***surveillance*** *de l'****espace*** *(Texte E 8141 - COM (2013) 107 final)*, N° 646, Sénat Session Ordinaire de 2012-2013, 10/06/13, [Online] http://www.senat.fr/leg/ppr12-646.pdf, Created: 10/06/13, Accessed: 18/06/13.

Giannopapa, C. and G. Oren (eds.) (2011) *Views on Public Perception and International Aspects of the European Space Flagship Programmes Galileo/EGNOS and GMES*, ESPI Report 33, Vienna: European Space Policy Institute.

Gleason, M. (2006) 'European Union Space Initiatives: The Political Will for Increasing European Space Power', *Astropolitics*, 4(1): 7-41.

Globalsecurity.org (2011a) 'Anti-Satellite Weapons – Overview', *Globalsecurity.org*, [Online] http://www.globalsecurity.org/space/systems/asat-overview.htm, Created: 21/07/11, Accessed: 24/09/12.

Globalsecurity.org (2011b) 'GPS III/ GPS Block III', *Globalsecurity.org*, [Online] http://www.globalsecurity.org/space/systems/gps_3.htm, Created: 21/07/11, Accessed: 01/05/12.

Gmes-mosaic.eu (2010) 'G-MOSAIC in a Nutshell', *G-MOSAIC GMES Pilot Services for Security – Project Overview*, [Online] http://www.gmes-gmosaic.eu/project-overview/19, Accessed: 20/03/13.

Gordon, M. R. and D. S. Cloud (2007) 'U.S. Knew of China's Missile Test, but Kept Silent', *The New York Times*, 23rd April 2007, [Online] http://www.nytimes.com/2007/04/23/washington/23satellite.html, Created: 23/04/07, Accessed: 20/08/13.

Gray, C. S. and G. Sloan (eds.) (1999) *Geopolitics Geography and Strategy*, London: Frank Cass.

Grego, L. (2012a) 'A History of Anti-Satellite Programs', *Union of Concerned Scientists*, [Online] http://www.ucsusa.org/assets/documents/nwgs/a-history-of-ASAT-programs_lo-res.pdf, Created: 31/01/12, Accessed: 25/09/12.

Grego, L. (2012b) 'Does a High-Altitude ASAT Test Make Sense', *Union of Concerned Scientists*, [Online] http://allthingsnuclear.org/does-a-high-altitude-asat-test-make-sense/, Created: 20/12/12, Accessed: 19/02/14.

Grego, L. and D. Wright (2010) *Securing the skies ten steps the United States should take to improve the security and sustainability of space*, Union of Concerned Scientists.

Grondin, D. (2012) 'The (power) politics of space the US astropolitical discourse of global dominance in the War on Terror' in: N. Bormann and M. Sheehan (eds.) *Securing Outer Space*, Abingdon: Routledge: 108-127.

Grusin, R. (2004) 'Premediation', *Criticism*, 46(1): 17-39.

Guillaume, X. (2013) ‘Criticality’ in: M. B. Salter and C. E. Multu (eds.) *Research Methods in Critical Security Studies An Introduction*, London: Routledge: 29-32.

Harris, A. and R. Harris (2006) ‘The need for air space and outer space demarcation’, *Space Policy*, 22 (1): 3-7.

Harris, R. (1987) *Satellite remote sensing An introduction*, London: Routledge & K. P.

Hartong, M., R. Goel and D. Wijesekera (2008) ‘Security and the US rail infrastructure’, *International Journal of Critical Infrastructure Protection*, 1(1): 15-28.

Havercroft, J. & R. Duvall (2012) 'Critical astropolitics The geopolitics of space control and the transformation of state sovereignty' in: N. Bormann and M. Sheehan (eds.) *Securing Outer Space*, Abingdon: Routledge: 42-58.

Hays, P. L. (2011) ‘Space Law and the Advancement of Spacepower’, [Online] http://www.ndu.edu/press/space-Ch28.html, Created:

Henri, Y. and V. Nozdrin (2012) ‘Economic methods of improving efficient use of the orbit/spectrum resource by satellite systems’, *Space Policy*, 28(3): 185-191.

Hercheui, M. D., D. Whitehouse, W. McIver Jr. and J. Phahlamohlaka (eds.) (2012) *ICT Critical Infrastructures and Society*, Heidelberg: Springer Berlin Heidelberg.

Hertzfeld, H. R. (2011) ‘Commercial Space and Spacepower’, [Online] http://www.ndu.edu/press/lib/pdf/spacepower/space-Ch5.pdf, Created: 06/06/11, Accessed: 16/06/13.

Hitchens, T. (2007) 'Debris, Traffic Management and Weaponization: Opportunities for and Challenges to Cooperation in Space', *Brown Journal of World Affairs*, 14 (1): 173-186.

HM Government (2014) *National Space Security Policy*, UKSA/13/1292 [Online] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/307346/National_Space_Security_Policy.pdf, Created: 30/04/14, Accessed: 08/05/14.

Hodder, I. (2003) ‘The Interpretation of Documents and Material Culture’ in: N. K. Denzin and Y. S. Lincoln (eds.) *Collecting and Interpreting Qualitative Materials*, Thousand Oaks: Sage Publications: 155-175.

Hoerlin, H. (1976) *United States High-Altitude Test Experiences A Review Emphasizing the Impact on the Environment*, Los Alamos, NM: Los Alamos Scientific Laboratory Monograph [Online] http://www.fas.org/sgp/othergov/doe/lanl/docs1/00322994.pdf, Accessed: 23/08/11.

Horikawa, Y. (2014) ‘ICoC and Long-Term Sustainability of Outer Space Activities’ in: R. P. Rajagopalan and D. A. Porras, *Awaiting Launch: Perspectives on the Draft ICOC for Outer Space Activities*, Observer Research Foundation [Online] http://orfonline.org/cms/export/orfonline/modules/report/attachments/AwaitingLaunch_1397728623369.pdf, Accessed: 17/04/14: 19-25

House of Commons Defence Committee (2012) *Developing Threats: Electro-Magnetic Pulses (EMP) Tenth Report of Session 2010-12*, HC 1552, London: The Stationery Office Limited.

Idziak, L. A. 'Cultural Resources Management in Outer Space: Historic Preservation in the Graveyard Orbits', *Sysesis A Journal of Science, Technology, Ethics, and Policy*, 4: G61-G75.

Inter-Agency Space Debris Coordination Committee (2007) *IADC Space Debris Mitigation Guidelines*, IADC – 02-01 Revision 1, Steering Group and Working Group 4.

Jakhu, R. (2007) 'Legal Issues of Satellite Telecommunications, the Geostationary Orbit, and Space Debris', *Astropolitics*, 5(2): 173-208.

Jakhu, R. and K. Singh (2009) 'Space Security and Competition for Radio Frequencies and Geostationary Slots', *Zeitschrift Für Luft-und Weltraumrecht*, 58(1): 74-93.

Jaramillo, C. (ed.) (2012) *Space Security Index 2012*, Project Ploughshares: Waterloo, Ontario.

Jensen, O. B. and T. Richardson (2004) *Making European Space mobility, power and territorial identity*, Abingdon: Routledge.

John A. Volpe National Transportation Centre (2001) *Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System Final Report*, [Online] http://www.navcen.uscg.gov/pdf/vulnerability_assess_2001.pdf, Created: 29/08/01, Accessed: 26/02/13.

Johnson, N. and E. Stansbery (2010) 'The new NASA orbital debris mitigation procedural requirements and standards', *Acta Astronautica*, 66(3-4): 362-367.

Johnson, N. L. (2004) 'Space traffic management: concepts and practices', *Space Policy*, 20(2): 79-85.

Johnson, R. E. (2006) *Europe's Space Policies and their relevance to the ESDP*, Brussels: European Parliament.

Johnson-Freese, J. (2006) 'A New US-Sino Space Relationship: Moving Toward Cooperation', *Astropolitics*, 4(2): 131-158.

Johnson-Freese, J. (2007) *Space as a Strategic Asset*, New York: Columbia University Press.

Johnson-Freese, J. (2009) *Heavenly Ambitions America's Quest to Dominate Space*, Philadelphia, University of Pennsylvania Press.

Joint Chiefs of Staff (2002) *Joint Doctrine for Space Operations*, Joint Publication 3-14, 9th August 2002, [Online] http://www.bits.de/NRANEU/others/jp-doctrine/jp3_14(02).pdf, Created: 30/07/02, Accessed: 05/10/12.

Joint Chiefs of Staff (2013a) *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication 1-02, 8th November 2010 (As Amended Through 15 June 2013) [Online] http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf, Created: 02/07/13, Accessed: 23/07/13.

Joint Chiefs of Staff (2013b) *Space Operations*, Joint Publication 3-14 29th May 2013, [Online] http://www.fas.org/irp/doddir/dod/jp3_14.pdf, Created: 05/06/13, Accessed: 23/07/13.

Jönsson, C., S. Tägil and G. Törnqvist (2000) *Organizing European Space*, London: Sage Publications Ltd.

Kan, S. (2007) 'China's Anti-Satellite Weapon Test', *Congressional Research Service*, [Online] http://www.fas.org/sgp/crs/row/RS22652.pdf, Created: 23/04/07, Accessed: 27/09/12.

Kaplan, C. (2009) 'The biopolitics of Technoculture in the Mumbai Attacks', *Theory, Culture and Society*, 26(7-8): 301-313.

Kaplan, E. D. and C. J. Hegarty (2006) *Understanding GPS Principles and Applications*, 2nd Edition, Norwood, MA: Artech House Inc.

Kessler, D. J. and B. G. Cour-Palais (1978) 'Collision Frequency of Artificial Satellites: The Creation of a Debris Belt', *Journal of Geophysical Research*, 83(A6): 2637-2646.

Klein, J. J. (2012) 'Space Strategy Considerations for Medium Space Powers', *Astropolitics*, 10(2): 110-125.

Kleinberg, H. (2007) 'On war in space', *Astropolitics*, 5(1): 1-27.

Klinkrad, H. (2007) 'On-orbit risk reduction – collision avoidance', *Proceedings of the Institution of Mechanical Engineers, Part G: Journal of Aerospace Engineering*, 221(6): 955-962.

Klinkrad, H. (2013) 'The Space Debris Environment Its Current State & Future Evolution', *Space Traffic Control – Is the Space Debris Problem Solvable? RAES Space Conference 2nd July 2013*, [Online] http://aerosociety.com/Assets/Docs/Events/718/(1)%20The%20Space%20Debris%20Problem.pdf, Accessed: 17/07/13.

Kohn, R. H. (2009) 'The Danger of Militarization in an Endless "War" on Terrorism, *The Journal of Military History*, 73(1): 177-208.

Koons, H. C., J. E. Mazur, R. S. Selesnick, J. B. Blake, J. F. Fennell, J. L. Roeder and P. C. Anderson (1999) *The Impact of the Space Environment on Space Systems*, TR-99(1670)-1, El Segundo, CA: The Aerospace Corporation Technology Operations [Online] http://klabs.org/richcontent/Reliability/space_environment/TR-99-1670-1.pdf, Accessed: 18/09/12.

Kramnik, I. (2009) ‘Is Russia ready for Star Wars?’, *RIANovosti – Features & Opinion*, [Online] http://en.rian.ru/analysis/20090812/155794013.html, Created: 12/08/2009, Accessed: 05/11/12.

Krepon, M., T. Hitchens and M. Katz-Hyman (2011) ‘Preserving Freedom of Action in Space: Realizing the Potential and Limits of U.S. Spacepower’, [Online] http://www.ndu.edu/press/lib/pdf/spacepower/space-Ch20.pdf, Created: 06/06/11, Accessed: 19/07/13.

Krige, J. and A. Russo (2000) *A History of the European Space Agency 1958-1987 Volume I The Story of ESRO and ELDO, 1958-1973*, Noordwijk: ESA Publications Division.

Krige, J., A. Russo and L. Sebesta (2000) *A History of the European Space Agency 1958-1987 Volume II The Story of ESA, 1973 to 1987*, Noordwijk: ESA Publications Division.

Lála, P. (2004) ‘Traffic Management Rules for Space Operations’, *Astropolitics*, 2(2): 121-132.

Lebeau, A. (1976) ‘The Changing Role of Europe in Space/La Mutation de l’Europe spatiale’, *ESA Bulletin*, 6: 3-5.

Lévy, J. (ed.) (2001) *From Geopolitics to Global Politics*, London: Frank Cass.

Lillesand, T. M. and R. W. Kiefer (1987) *Remote Sensing and Image Interpretation*, Second Edition, New York: John Wiley & Sons.

Lindström, G. and G. Gasparini (2003) ‘The Galileo satellite system and its security implications’, *Occasional Papers*, no. 44, Paris: The European Union Institute for Security Studies.

Lintz, J. and D. S. Simonett (1976a) ‘Preface and Introduction’ in: J. Lintz and D. S. Simonett (eds.) *Remote Sensing of the Environment*, Reading, MA: Addison-Wesley Publishing Company: 1-9.

Lintz J. and D. S. Simonett (eds.) (1976b) *Remote Sensing of the Environment*, Reading, MA: Addison-Wesley Publishing Company.

Listner, M. (2012a) ‘A new paradigm for arbitrating disputes in outer space’, *The Space Review essays and commentaries about the final frontier*, [Online] http://www.thespacereview.com/article/2002/1, Created: 09/01/12, Accessed: 10/01/12.

Listner, M. (2012b) ‘Geopolitical Challenges to Implementing the Code of Conduct for Outer Space Activities’, *e-International Relations*, [Online] http://www.e-ir.info/2012/06/26/geopolitical-challenges-to-implementing-the-code-of-conduct-for-outer-space-activities/, Created: 26/06/12, Accessed: 07/01/12.

Listner, M. (2012c) ‘Iridium 33 and Cosmos 2251 three years later: where are we now? *The Space Review essays and commentaries about the final frontier*, [Online] http://www.thespacereview.com/article/2023/1, Created: 13/02/12, Accessed: 04/10/12.

Listner, M. (2013) ‘Separation of powers battle continues over the Code of Conduct’, *The Space Review essays and commentaries about the final frontier*, [Online] http://www.thespacereview.com/article/2215/1, Created: 07/01/13, Accessed: 19/08/13.

Lobo-Guerrero, L. (2013a) ‘Archives’ in: M. B. Salter and C. E. Multu (eds.) *Research Methods in Critical Security Studies An Introduction*, London: Routledge: 121-124.

Lobo-Guerrero, L. (2013b) ‘Wondering as a research attitude’ in: M. B. Salter and C. E. Multu (eds.) *Research Methods in Critical Security Studies An Introduction*, London: Routledge: 25-28.

Lukes, S. (ed.) (1994) *Power*, Oxford: Blackwell Publishers.

Lukes, S. (2005) *Power A Radical View*, Second Edition, Basingstoke: Palgrave MacMillan.

Lum, G. K., N. R. Bennett and J. M. Lockhart (1997) ‘System Hardening Approaches for a LEO Satellite With Radiation Tolerant Parts’, *IEEE Transactions on Nuclear Science*, 44(6): 2026-2033.

Lutes, C. D., P. L. Hays, V. A. Manzo, L. M. Yambrick and M. E. Bunn (eds.) (2011a) *Toward a Theory of Spacepower Selected Essays*, Washington, D.C.: National Defense University Press.

Lutes, C. D., P. L. Hays, V. A. Manzo, L. M. Yambrick and M. E. Bunn (2011b) ‘Introduction’ in: Lutes, C. D., P. L. Hays, V. A. Manzo, L. M. Yambrick and M. E. Bunn (eds.) (2011a) *Toward a Theory of Spacepower Selected Essays*, Washington, D.C.: National Defense University Press: xiii-xx.

MacDonald, F. (2007) ‘Anti-Astropolitik outer space and the orbit of geography’, *Progress in Human Geography*, 31(5): 592-615.

MacDonald, F., R. Hughes and K. Dodds (eds.) (2010b) *Observing States Geopolitics and Visual Culture*, I. B. Tauris & Co. Ltd.

Madders, K. J. and W. M. Thiebaut (1992) ‘Two Europes in One Space: The Evolution of Relations Between the European Space Agency and the European Community in Space Affairs’, *Journal of Space Law*, 20: 117-132.

Marks, P. (2009) ‘Satellite collision “more powerful than China’s ASAT test”’, *New Scientist Space*, [Online] http://www.newscientist.com/article/dn16604-satellite-collision-more-powerful-than-chinas-asat-test.html, Created: 13/02/09, Accessed: 04/10/12.

Marta, L. (2013) ‘National visions of European space governance: Elements for a new institutional architecture”, *Space Policy*, 29(1): 20-27.

Martin, A., M. Couston and L. Ravillon (2009) *Galileo Chronique d’une politique spatiale européenne annoncée*, Paris: LexisNexis.

Martino, J. (2012) ‘Video Games and the Militarisation of Society: Towards a Theoretical and Conceptual Framework’ in: M. D. Hercheui, D. Whitehouse, W. McIver Jr. and J. Phahlamohlaka (eds.) *ICT Critical Infrastructures and Society*, Heidelberg: Springer Berlin Heidelberg: 264-273.

Massumi, B. (2007) ‘Potential politics and the primacy of preemption’, *Theory & Event*, 10(2), [Online] http://muse.jhu.edu/journals/theory_and_event/v010/10.2massumi.html, Accessed: 04/07/13.

Mathieu, C. (2010) ‘Assessing Russia’s space cooperation with China and India – Opportunities and challenges for Europe’, *Acta Astronautica*, 66(3-4): 355-361.

McCarthy, J. A. (2007) ‘Introduction From Protection to Resilience: Injecting “Moxie” Into the Infrastructure Security Continuum’ in: J. A. McCarthy, C. Pommerening, L. J. Perelman, P. L. Scalingi, D. A. Garbin, J. F. Shortle, D. Arsenault, A. Sood, D. B. Moody, E. M. Jackson, *Critical Thinking: Moving from Infrastructure Protection to Infrastructure Resilience*, George Mason University CIP Program Discussion Paper Series: 1-7.

McCarthy, J. A., C. Pommerening, L. J. Perelman, P. L. Scalingi, D. A. Garbin, J. F. Shortle, D. Arsenault, A. Sood, D. B. Moody, E. M. Jackson (2007) *Critical Thinking: Moving from Infrastructure Protection to Infrastructure Resilience*, George Mason University CIP Program Discussion Paper Series.

Meek, P. A. (2012) ‘The CPR approach to space sustainability: Commentaries on Weeden and Chow’, *Space Policy*, 28(3): 173-176.

Metzger, J. (2004) ‘The Concept of Critical Infrastructure Protection (CIP)’ in: A. J. K. Bailes and I. Frommelt (eds.) *Business and Security: Public-Private Sector Relationships in a New Security Environment*, Oxford: Oxford University Press: 197-209.

Milowicki, G. V. and J. Johnson-Freese (2008) ‘Strategic Choices: Examining the United States military response to the Chinese Anti-satellite test’, *Astropolitics*, 6(1): 1-21.

Mineiro, M. C. (2008) ‘*FY-1C* and *USA-193* ASAT intercepts: An assessment of legal obligations under Article IX of the Outer Space Treaty’, *Journal of Space Law*, 34(2): 321-356.

Ministry of Defence (2012) *Protecting access to space*, Multinational Experiment (MNE) 7, [Online] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/28680/20121204mne7_protecting_access.pdf, Created: 08/12/12, Accessed: 24/07/13.

Moltz, J. C. (2008) *The Politics of Space Security Strategic Restraint and the Pursuit of National Interests*, Stanford, CA: Stanford University Press.

Moore, M. (2005) ‘Space war – now we’re jammin’!’, *Bulletin of Atomic Scientists*, March/April: 6-8.

Müller, M. (2010) ‘Doing discourse analysis in Critical Geopolitics’, *L’Espace Politique*, 12(3): 1-21.

Mutschler, M. M. and C. Venet (2012) ‘The European Union as an emerging actor in space security?’ *Space Policy*, 28(2): 118-124.

Nardon, L. and C. Venet (2011) ‘GMES, the second flagship’, *Europe and Space Series*, 11: 1-6.

NASA Near Earth Object Program (2013) ‘Frequently Asked Questions’, *National Space and Aeronautics Administration Near Earth Object Program*, [Online] http://neo.jpl.nasa.gov/faq/#pha, Created: 18/06/13, Accessed: 18/06/13.

NASA Orbital Debris Program Office (2005) ‘Accidental Collisions of Catalogued Satellites Identified’, *Orbital Debris Quarterly News*, 9(2): 1-2.

NASA Orbital Debris Program Office (2009) ‘Satellite Collision Leaves Significant Debris Clouds’, *Orbital Debris Quarterly News*, 13(2): 1-2.

NASA Orbital Debris Program Office (2012a) ‘Increase in ISS Debris Avoidance Maneuvers’, *Orbital Debris Quarterly News*, 16(2): 1-2.

NASA Orbital Debris Program Office (2012b) ‘Status of Three Major Debris Clouds’, *Orbital Debris Quarterly News*, 16(3): 2.

National Aeronautics and Space Administration (1995) *NASA Safety Standard Guidelines and Assessment Procedures for Limiting Orbital Debris*, Washington D.C.: NASA Office of Safety and Mission Assurance.

National Aeronautics and Space Administration (2009) *Process for Limiting Orbital Debris*, NASA-STD 8719.14, Washington D.C.: National Aeronautics and Space Administration.

National Aeronautics and Space Administration (2012) ‘SOHO’s Orbit’, *SOHO Solar and Heliospheric Observatory*, [Online] http://soho.nascom.nasa.gov/about/orbit.html, Created: 17/01/12, Accessed: 17/09/12.

National Aeronautics and Space Administration (2013) ‘Solar Sail Demonstrator’, *Technology Demonstration Missions*, [Online] http://www.nasa.gov/mission_pages/tdm/solarsail/solarsail_overview.html, Created: 30/10/13, Accessed: 19/02/14.

National Aeronautics and Space Administration Goddard Flight Center (2000) *COSPAS-SARSAT Search and Rescue System*, LG 2000-XX-XXX-GSFC, [Online] http://www.nasa.gov/centers/goddard/pdf/105930main_cospas.pdf, Created: 17/11/00, Accessed: 18/12/12.

National Security Council (1955) *NSC 5520 Statement of Policy on U.S. Scientific Satellite Program 20th May 1955*, [Online] http://www.marshall.org/pdf/materials/805.pdf, Created: 20/04/10, Accessed: 31/10/12.

Necesal, L., L. Lukas and R. Jasek (2011) ‘Measures for Critical Infrastructure Protection in the Czech Republic’, *Annals of DAAAM for 2011 & Proceedings of the 22nd International DAAAM Symposium*, 22(1): 843-845.

Nickolov, E. (2005) ‘Critical Information Infrastructure Protection: Analysis, Evaluation and Expectations’, *Information & Security: An International Journal*, 17: 105-119.

Norris, P. (2010) *Watching Earth from Space how surveillance helps us – and harms us*, Chichester: Praxis Publishing.

North Atlantic Treaty Organisation (2010) ‘Official Text: Active Engagement, Modern Defence Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation adopted by Heads of State and Government in Lisbon’, [Online] http://www.nato.int/cps/en/natolive/official_texts_68580.htm, Created: 19/11/10, Accessed: 25/08/11.

O’Hanlon, M. E. (2004) *Neither Star Wars nor Sanctuary Constraining the Military Uses of Space*, Washington D.C.: Brookings Institution Press.

Ó Tuathail, G. (1994) ‘(Dis)placing geopolitics: writing on the maps of global politics’, *Environment and Planning D: Society and Space*, 12(5): 525-546.

Ó Tuathail, G. (1996) *Critical Geopolitics*, London: Routledge.

Ó Tuathail, G. (1998) ‘Postmodern Geopolitics? The modern geopolitical imagination and beyond’ in: G. Ó Tuathail and S. Dalby (eds.) *Rethinking Geopolitics*, London: Routledge: 16-38.

Ó Tuathail, G. (1999) ‘Understanding Critical Geopolitics: Geopolitics and Risk Society’ in: C. S. Gray and G. Sloan (eds.) *Geopolitics Geography and Strategy*, London: Frank Cass: 107-124.

Ó Tuathail, G. (2002) ‘Theorizing practical geopolitical reasoning: the case of the United States’ response to the war in Bosnia’, *Political Geography*, 21(5): 601-628.

Ó Tuathail, G. (2010) ‘Localizing geopolitics: Disaggregating violence and return in conflict regions’, *Political Geography*, 29(5): 256-265.

Ó Tuathail, G. and S. Dalby (1998a) ‘Introduction: Rethinking Geopolitics Towards a critical geopolitics’ in: G. Ó Tuathail and S. Dalby (eds.) *Rethinking Geopolitics*, London: Routledge: 1-15.

Ó Tuathail, G. and S. Dalby (eds.) (1998b) *Rethinking Geopolitics*, London: Routledge.

Oberg, J. (1999) *Space Power Theory*, US Air Force Academy.

Oberg, J. (2003) ‘Toward a Theory of Space Power: Defining Principles for U.S. Space Policy’, [Online] http://www.marshall.org/pdf/materials/140.pdf, Created: 14/07/2003, Accessed: 12/09/11.

Odenwald, S., J. Green and W. Taylor (2006) ‘Forecasting the impact of an 1859-calibre superstorm on satellite resources’, *Advances in Space Research*, 38(2): 280-297.

Odenwald, G. (2003) ‘The Never Ending Dispute: Legal Theories on the Spatial Demarcation Boundary Plane between Airspace and Outer Space’, *Hertfordshire Law Journal*, 1(2): 64-84.

Oduntan, G. (2012) *Sovereignty and Jurisdiction in the Airspace and Outer Space Legal Criteria for Spatial Delimitation*, Abingdon: Routledge.

Ofcom (2013) ‘Frequency planning and licensing’, *Ofcom – Frequency Planning*, [Online] http://licensing.ofcom.org.uk/radiocommunication-licences/regulations-technical-reference/rules/policy-manual/freq_planning, Accessed: 23/07/13.

Oikonomou, I. (2012) ‘The European Defence Agency and EU military space policy: Whose space odyssey?’, *Space Policy*, 28(2): 102-109.

Operationally Responsive Space Office (2013) ‘Mission’, *Operationally Responsive Space*, [Online] http://ors.csd.disa.mil/mission/, Created: 21/02/13, Accessed: 19/06/13.

Orr, J. (2004) ‘The Militarization of Inner Space’, *Critical Sociology*, 30(2): 451-481.

Outer Space Act (1986) Chapter 38, London: Her Majesty’s Stationary Office.

Pace, S., G. Frost, I. Lachow, D. Frelinger, D. Fossum, D. K. Wassem and M. Pinto (1995) *The Global Positioning System Assessing National Policies*, Santa Monica, CA: RAND.

Paglen, T. (2011) ‘The Other Night Sky’, *Trevor Paglen – Work*, [Online] http://www.paglen.com/?l=work&s=othernightsky, Accessed: 15/08/13.

Pape, R. A. (1996) *Bombing to Win Air Power and Coercion in War*, New York: Cornell University Press.

Pardini, C. and L. Anselmo (2009) ‘USA-193 decay predictions using public domain trajectory data and assessment of the post-intercept orbital debris cloud’, *Acta Astronautica*, 64(7-8): 787-795.

Parker, N. (2010) ‘Empire as Geopolitical Figure’, *Geopolitics*, 15(1): 109-132.

Parry, J. H. (1973) *The Age of Reconnaissance Discovery, Exploration and Settlement 1450-1650*, London: Cardinal.

Pasco, X. (2009) *A European Approach to Space Security*, Cambridge, MA: American Academy of Arts and Sciences.

Pasco, X. (2011) ‘The European “Spacepower”? A Multifaceted Concept’, [Online] http://www.ndu.edu/press/lib/pdf/spacepower/space-Ch25.pdf, Created: 18/05/11, Accessed: 16/06/13.

Pasco, X. (2014) 'ICoC: An Imperfect but Necessary Step?' in: R. P. Rajagopalan and D. A. Porras, *Awaiting Launch: Perspectives on the Draft ICOC for Outer Space Activities*, Observer Research Foundation [Online] http://orfonline.org/cms/export/orfonline/modules/report/attachments/AwaitingLaunch_1397728623369.pdf, Accessed: 17/04/14: 95-100.

Pavelec, S. M. (2012) 'The Inevitability of the Weaponization of Space: Technological Constructivism Versus Determinism', *Astropolitics*, 10(1): 39-48.

Peoples, C. (2008) 'Assuming the Inevitable? Overcoming the Inevitability of Outer Space Weaponization and Conflict', *Contemporary Security Policy*, 29(3): 502-520.

Peoples, C. (2010) 'The growing 'securitization' of outer space, *Space Policy*, 26(4): 205-208.

Peoples, C. (2011) 'The Securitization of Outer Space: Challenges for Arms Control', *Contemporary Security Policy*, 32(1): 76-98.

Perelman, L. J. (2007) 'Shifting Security Paradigms: Toward Resilience' in: J. A. McCarthy, C. Pommerening, L. J. Perelman, P. L. Scalingi, D. A. Garbin, J. F. Shortle, D. Arsenault, A. Sood, D. B. Moody, E. M. Jackson, *Critical Thinking: Moving from Infrastructure Protection to Infrastructure Resilience*, George Mason University CIP Program Discussion Paper Series: 23-48.

Peter, N. (2005) 'Space and Security: The Emerging Role of Europe', *Astropolitics*, 3(3): 265-296.

Peter, N. (2010) 'Space power and its implications – The case of Europe', *Acta Astronautica*, 66(3-4): 348-354.

Pfaltzgraff, R. L. and J. L. Deghand (1968) 'European Technological Collaboration: The Experience of the European Launcher Development Organization (ELDO)', *Journal of Common Market Studies*, 7(1): 22-34.

Pfaltzgraff Jr., R. L. (2011) 'International Relations Theory and Spacepower', in: Lutes, C. D., P. L. Hays, V. A. Manzo, L. M. Yambrick and M. E. Bunn (eds.) (2011a) *Toward a Theory of Spacepower Selected Essays*, Washington, D.C.: National Defense University Press: 37-56.

Pommerening, C. (2007) 'Resilience in Organizations and Systems. Background and Trajectories of an Emerging Paradigm' in: J. A. McCarthy, C. Pommering, L. J. Perelman, P. L. Scalingi, D. A. Garbin, J. F. Shortle, D. Arsenault, A. Sood, D. B. Moody, E. M. Jackson, *Critical Thinking: Moving from Infrastructure Protection to Infrastructure Resilience*, George Mason University CIP Program Discussion Paper Series: 9-21.

Portelli, C., F. Alby, R. Crowther and U. Wirt (2010) 'Space Debris Mitigation in France, Germany, Italy and United Kingdom', *Advances in Space Research*, 45(8): 1035-1041.

President's Commission on Critical Infrastructure Protection (1997) *Critical Foundations Protecting America's Infrastructures The Report of the President's Commission on Critical Infrastructure Protection*, [Online] http://www.fas.org/sgp/library/pccip.pdf, Created: 22/04/05, Accessed: 08/12/11.

Prieto, R. (2003) 'Business community views', *Technology in Society*, 25(4): 517-522.

Prior, L. (2003) *Using Documents in Social Research*, London: Sage Publications.

Pursiainen, C. (2009) 'The Challenges for European Critical Infrastructure Protection', *European Integration*, 31(6): 721-739.

Rajagopalan, R. P. and D. A. Porras (2014) *Awaiting Launch: Perspectives on the Draft ICOC for Outer Space Activities*, Observer Research Foundation [Online] http://orfonline.org/cms/export/orfonline/modules/report/attachments/AwaitingLaunch_1397728623369.pdf, Accessed: 17/04/14.

Rathgeber, W., N.-L. Remuss and K.-U. Schrogl (2009) 'Space Security and the European Code of Conduct for Outer Space Activities' in: United Nations Institute for Disarmament Research, *Disarmament Forum No. 4 – A Safer Space Environment?*, UNIDIR/2009/14, Geneva: United Nations: 33-41.

Remuss, N.-L. (2009) *Space and Internal Security – Developing a Concept for the Use of Space Assets to Assure a Secure Europe*, ESPI Report 20, Vienna: European Space Policy Institute.

Rendleman, J. D. (2010) 'Lawful Response to Attacks on Space Systems', *Space and Defense*, 4(1): 3-52.

République Française (2013) *Loi n° 2008-518 du 3 Juin 2008 relative aux opérations spatiales*, [Online] http://legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000018931380, Created: 30/05/13, Accessed: 08/07/13.

Retaillé, D. (2001) 'Geopolitics in History' in: Lévy, J. (ed.) *From Geopolitics to Global Politics*, London: Frank Cass: 35-51.

Reuters (2012) 'US Air Force Begins Using Boeing Surveillance Satellite', *Aviation Week Defense*, [Online] http://www.aviationweek.com/Article.aspx?id=/article-xml/awx_08_21_2012_p0-488015.xml, Created: 21/08/12, Accessed: 05/09/12.

Rex, D. (1998) 'Space debris mitigation and space systems design', *Acta Astronautica*, 41(4): 311-316.

RIA Novosti (2009) 'Russia to revamp air-space defenses by 2020 – Air Force Chief' *RIA Novosti – Defense*, [Online] http://en.rian.ru/mlitary_news/20090811/155782307.html, Created: 11/08/09, Accessed: 05/11/12.

RIA Novosti (2010) ‘Russian officer says developing new weapon for space defense’, *RIA Novosti – Russia*, [Online] http://en.rian.ru/russia/20100515/159029349.html, Created: 15/05/10, Accessed: 01/11/12.

Richardson, T. (2006) ‘The Thin Simplifications of European Space: Dangerous Calculations?’, *Comparative European Politics*, 4(2-3): 203-217.

Roberts, L. D. (2000) ‘A lost connection: Geostationary satellite networks and the International Telecommunications Union’, *Berkeley Technology Law Journal*, 15(3): 1095-1144.

Robinson, J. (2010) *The Role of Transparency and Confidence-Building Measures in Advancing Space Security*, ESPI Report 28, Vienna: European Space Policy Institute.

Robinson, J. (2011a) ‘Advancing Key Foreign Policy Objectives Via Space: Europe Case Study’, *Proceedings of the 62nd IAC, International Astronautical Congress*, IAC-11-E3.1.2.

Robinson, J. (2011b) *Enabling Europe’s Key Foreign Policy Objectives Via Space*, ESPI Report 30, Vienna: European Space Policy Institute.

Robinson, J. (2011c) ‘Transparency and confidence-building measures for space security’, *Space Policy*, 27(1): 27-37.

Robinson, J. (2012) ‘Advancing an International Space Code of Conduct’, *e-International Relations*, [Online] http://www.e-ir.info/2012/07/13/transparency-and-confidence-building-measures-as-practical-tools-for-advancing-an-international-space-code-of-conduct/, Created: 13/07/12, Accessed: 13/07/12.

Royal Academy of Engineering (2013) *Extreme space weather: impacts on engineered systems and infrastructure*, London: Royal Academy of Engineering.

Russell, B. (1994) ‘The Forms of Power’ in: S. Lukes (ed.) *Power*, Oxford: Blackwell Publishers: 19-27.

Russo, A. (2000) ‘The Beginning of the Telecommunications Satellite Programmes in ESRO’ in: J. Krige and A. Russo, *A History of the European Space Agency 1958-1987 Volume I The Story of ESRO and ELDO, 1958-1973*, Noordwijk: ESA Publications Division: 253-298.

Sachdeva, G. S. (2009) ‘Space Mines: Dialectics of Legality’, *Astropolitics*, 7(2): 135-149.

Sadeh, E. (2011) ‘Spacepower and the environment’, [Online] http://www.ndu.edu/press/lib/pdf/spacepower/space-Ch13.pdf, Created: 18/05/11, Accessed: 24/06/13.

Said, E. W. (1993) *Culture and Imperialism*, London: Chatto & Windus.

Said, E. W. (2003) *Orientalism*, London: Penguin.

Salter, M. B. and C. E. Multu (eds.) (2013) *Research Methods in Critical Security Studies An Introduction*, London: Routledge.

Satnews.com (2012) 'Surrey Satellite Technology Ltd. (SSTL)… Retiring, Yet Remaining Operational', *Satnews.com Satnews Daily* [Online] http://www.satnews.com/cgi-bin/story.cgi?number=1557778556, Created: 08/07/12, Accessed: 25/07/12.

Scalingi, P. L. (2007) 'Moving Beyond Critical Infrastructure Protection to Disaster Resilience' in: J. A. McCarthy, C. Pommerening, L. J. Perelman, P. L. Scalingi, D. A. Garbin, J. F. Shortle, D. Arsenault, A. Sood, D. B. Moody, E. M. Jackson, *Critical Thinking: Moving from Infrastructure Protection to Infrastructure Resilience*, George Mason University CIP Program Discussion Paper Series: 49-71.

Schmitt, C. (2006) *The Nomos of the Earth in the International Law of Jus Publicum Europaeum*, Translated by G. L. Ulmen, New York: Telos Press Publishing.

Seed, P. (1998) *Ceremonies of Possession in the Europe's Conquest of the New World 1492-1640*, Cambridge: Cambridge University Press.

Sénat (2013) *Résolution Européenne sur la* ***surveillance*** *de l'****espace*** *(E 8141)*, N° 194 Sénat Session Extraordinaire de 2012-2013, 16/07/13, [Online] http://www.senat.fr/leg/tas12-194.pdf, Created 16/07/13, Accessed: 17/08/13.

Sgobba, T. (2008) 'An International Civil Aviation Organization for Outer Space?' in: United Nations Institute for Disarmament Research, *Security in Space The Next Generation Conference Report 31 March – 1 April 2008*, UNIDIR/2008/14, Geneva: United Nations Institute for Disarmament Research: 103-120.

Shanker, T. (2008) 'Missile Strikes a Spy Satellite Falling From Its Orbit', *The New York Times*, [Online] http://www.nytimes.com/2008/02/21/us/21satellite.html, Created: 21/02/08, Accessed: 27/09/12.

Shaw, M. N. (2003) *International Law*, 5th Edition, Cambridge: Cambridge University Press.

Sheehan, M. (2007) *The International Politics of Space*, Abingdon: Routledge.

Sheehan, M. (2011) 'EU Strategy, CSDP and the European Space Programme', *Studia Diplomatica – The Brussels Journal of International Relations*, LXIV(1): 41-53.

Sheehan, M. (2012) 'Profaning the path to the sacred The militarisation of the European Space Programme' in: N. Bormann and M. Sheehan (eds.) *Securing Outer Space*, Abingdon: Routledge: 170-185.

Sheldon, J. B. and C. S. Gray (2011) 'Theory Ascendant? Spacepower and the Challenge of Strategic Theory' in: C. D. Lutes, P. L. Hays, V. A. Manzo, L. M. Yambrick and M. E. Bunn (eds.) *Toward a Theory of Spacepower Selected Essays*, Washington, D.C.: National Defense University Press: 1-17.

Shue, H. and D. Rodin (2010a) ‘Introduction’ in: H. Shue and D. Rodin (eds.) *Preemption Military Action and Moral Justification*, Oxford: Oxford University Press: 1-22.

Shue, H. and D. Rodin (eds.) (2010b) *Preemption Military Action and Moral Justification*, Oxford: Oxford University Press.

Simmel, G. (1994) ‘Domination and Freedom’ in: S. Lukes (ed.) *Power*, Oxford: Blackwell Publishers: 203-210.

Slijper, F. (2008) *From Venus to Mars The European Union’s steps towards the militarisation of space*, Transnational Institute, [Online] http://www.tni.org/sites/www.tni.org/files/download/venustomars.pdf, Created: 10/11/08, Accessed: 20/08/13.

Sokolow, J. A. (2003) *The Great Encounter Native Peoples and European Settlers in the Americas, 1492-1800*, New York: M. E. Sharpe.

Spacenews.com (2012) ‘Battle Brewing Between ESA and EU Over Space Policy, Budget Authority’, *spacenews.com – Civil Space*, [Online] http://www.spacenews.com/article/battle-brewing-between-esa-and-eu-over-space-policy-budget-authority, Created: 30/11/12, Accessed: 05/12/12.

Spacy II, W. (2003) ‘Assessing the military utility of space-based weapons’, *Astropolitics*, 1(3): 1-43.

Sparke, M. (2007) ‘Geopolitical Fears, Geoeconomic Hopes, and the Responsibilities of Geography’, *Annals of the Association of American Geographers*, 97(2): 338-349.

Speakes, L. M. (2009) ‘Statement by Deputy Press Secretary Speakes on the Soviet Attack on a Korean Civilian Airliner September 16, 1983’ [Online] http://www.reagan.utexas.edu/archives/speeches/1983/91683c.htm, Created: 06/10/09, Accessed: 10/12/12.

Stares, P. B. (1985) *The Militarization of Space U.S. Policy, 1945-1984*, Ithaca: Cornell University Press.

Steinberg, A. (2012) ‘Weapons in Space: The Need to Protect Space Assets’, *Astropolitics*, 10(3): 248-267.

Steinberg, P. (2012) ‘The Shape of Things to Come (or Things that Were): Revisiting Politomorphology’, *Geopolitics & Security Critical Perspectives from Royal Holloway*, [Online] http://rhulgeopolitics.wordpress.com/2012/06/06/the-shape-of-things-to-come-or-things-that-were-revisiting-politomorphology/, Created: 06/06/12, Accessed: 19/08/13.

Steinberg, P. E. (2001) *The Social Construction of the Ocean*, Cambridge: Cambridge University Press.

Stern, J. and J. B. Wiener (2006) ‘Precaution Against Terrorism’, *Journal of Risk Research*, 9(4): 393-447.

Stoker, L. (2012) ‘Does the Earth need a space fence? Being hit by space junk is rubbish’, *Thenewstatesman.com The Business End*, [Online] http://www.newstatesman.com/blogs/business-blog/2012/10/does-earth-need-space-fence, Created: 04/10/12, Accessed: 04/10/12.

Strachan, H. (2010) ‘Preemption and Prevention in Historical Perspective’ in: H. Shue and D. Rodin (eds.) *Preemption Military Action and Moral Justification*, Oxford: Oxford University Press: 23-39.

Stuart, J. (2012) 'Unbundling sovereignty, territory and the state in outer space Two approaches' in: N. Bormann and M. Sheehan (eds.) *Securing Outer Space*, Abingdon: Routledge: 8-23.

Suzuki, K. (2003) *Policy Logics and Institutions of European Space Collaboration*, Aldershot: Ashgate.

The Economist (2010) ‘Satellite wars: Endangered birds’, *The Economist*, [Online] http://www.economist.com/node/17647639, Created 09/12/10, Accessed: 08/05/14.

The European Parliament and the Council of the European Union (2006) ‘Decision No 1982/2006/EC of the European Parliament and of the Council of 18 December 2006 concerning the Seventh Framework Programme of the European Community for research, technological development and demonstration activities (2007-2013)’, *Official Journal of the European Union*, 30/12/06: L 412/1-L 412/41.

The European Parliament and the Council of the European Union (2013) ‘Regulation (EU) No 1285/2013 of the European Parliament and of the Council on the implementation and exploitation of European satellite navigation systems and repealing Council Regulation (EC) No 876/2002 and Regulation (EC) No 683/2008 of the European Parliament and of the Council’, *Official Journal of the European Union*, 20/12/13: L 347/1-L 347/24.

The European Parliament and the Council of the European Union (2014a) ‘Decision No 541/2014/EU of the European Parliament and of the Council of 16 April 2014 establishing a Framework for Space Surveillance and Tracking Support’, *Official Journal of the European Union*, 27/05/2014: L 158/227-L 158/234.

The European Parliament and the Council of the European Union (2014b) ‘Regulation (EU) No 377/2014 of the European Parliament and of the Council of 3 April 2014 establishing the Copernicus Programme and repealing Regulation (EU) No 911/2010’, *Official Journal of the European Union*, 24/04/14: L 122/44-L 122/66.

Todorov, T. (1992) *The Conquest of America The Question of the Other*, Translated by Richard Howard, New York: HarperPerennial.

Topychkanov, P. (2010) ‘Features of the Outer Space Environment’ in: A. Arbatov and V. Dvorkin (eds.) *Outer Space Weapons, Diplomacy, and Security*, Washington D.C.: Carnegie Endowment for International Peace: 3-15.

Trimble, C. R. (2003) ‘Phantom Menace’, *Foreign Affairs*, [Online] http://www.foreignaffairs.com/articles/59197/charles-r-trimble/phantom-menace, Accessed: 20/03/12.

United Kingdom Space Agency (2013) ‘The Outer Space Act 1986’, *UK Space Agency – UK capabilities for overseas markets*, [Online] http://www.bis.gov.uk/ukspaceagency/what-we-do/space-and-the-growth-agenda/uk-capabilities-for-overseas-markets/the-outer-space-act-1986, Created: 16/01/13, Accessed: 11/02/13.

United Nations (2002) *United Nations Treaties and Principles on Outer Space Text of treaties and principles governing the activities of States in the exploration and use of outer space, adopted by the United Nations General Assembly*, ST/SPACE/11, New York: United Nations.

United Nations General Assembly (2006) *Transparency and confidence-building measures in outer space activities*, A/RES/61/75, New York: United Nations.

United Nations Office for Outer Space Affairs (2010) *Space Debris Mitigation Guidelines of the Committee on the Peaceful Uses of Outer Space*, Vienna: United Nations.

United States Air Force (1997) *Air Force Doctrine Basic Doctrine*, Air Force Doctrine Document 1, September 1997, [Online] http://www.fas.org/man/dod-101/usaf/docs/afdd/afdd1.pdf, Created: 30/03/1999, Accessed: 05/10/12.

United States Air Force (2011) *Air Force Basic Doctrine, Organization, and Command*, Air Force Doctrine Document 1, 14th October 2011, [Online] http://www.e-publishing.af.mil/shared/media/epubs/AFDD1.pdf, Created: 14/10/11, Accessed: 05/10/12.

United States Congress (2012) *National Defense Authorization Act for Fiscal Year 2013*, [Online] http://www.gpo.gov/fdsys/pkg/BILLS-112hr4310enr/pdf/BILLS-112hr4310enr.pdf, Created: 28/12/12, Accessed: 08/01/13.

United States Department of Homeland Security (2012) ‘Critical Infrastructure Protection’, *Homeland Security*, [Online] http://www.dhs.gov/critical-infrastructure-sectors, Accessed: 03/01/12.

United States General Accounting Office (2002) *Critical Infrastructure Protection Commercial Satellite Security Should Be More Fully Addressed*, GAO-02-781, Washington, D.C.: United States General Accounting Office, [Online] http://www.gao.gov/new.items/d02781.pdf, Created: 30/08/02, Accessed: 25/02/13.

United States Government (1997) *U.S. Government Orbital Debris Mitigation Standard Practices*, [Online] http://orbitaldebris.jsc.nasa.gov/library/USG_OD_Standard_Practices.pdf, Created: 01/10/04, Accessed: 06/08/13.

United States House of Representatives (2012) *National Defense Authorization Act for Fiscal Year 2013 Report of the Committee on Armed Services House of Representatives on H.R. 4310 Together with Additional and Dissenting Views*, Washington, D.C.: U.S.

Government Printing Office, [Online] http://www.gpo.gov/fdsys/pkg/CRPT-112hrpt479/pdf/CRPT-112hrpt479.pdf, Created: 02/01/13, Accessed: 07/01/13.

United States National Space Weather Program (2011) ‘Agency Participants’, *NSWP.gov*, [Online] http://www.nswp.gov/, Created: 28/09/11, Accessed: 05/09/12.

Vogler, J. (2000), *The Global Commons Environmental and Technological Governance*, Chichester: John Wiley & Sons, Ltd.

von der Dunk, F. (2010) ‘Europe and Security Issues in Space: The Institutional Setting’, *Space and Defense*, 4(1): 71-99.

Von Prittwitz, V. (2011) *ESPI Perspectives 50 Space as Environment: On the Way to Sustainable Space Policy*, Vienna: European Space Policy Institute.

Wang, S.-C. (2009) ‘The Making of New ‘Space’: Cases of Transatlantic Astropolitics’, *Geopolitics*, 14(3): 433-461.

Webb, D. (2012) ‘Space Weapons Dream, Nightmare or Reality?’ in: N. Bormann and M. Sheehan (eds.), *Securing Outer Space*, Abingdon: Routledge: 24-41.

Weeden, B. (2013) *Anti-Satellite Tests in Space – The Case of China*, [Online] http://swfound.org/media/115643/China_ASAT_Testing_Fact_Sheet_Aug2013.pdf, Created: 29/08/13, Accessed: 19/02/14.

Weeden, B. C. and T. Chow (2012) ‘Taking a common-pool resources approach to space sustainability: A framework and potential policies’, *Space Policy*, 28(3): 166-172.

White House (2006) *U.S. National Space Policy*, http://www.fas.org/irp/offdocs/nspd/space.pdf, Created: 9/10/06, Accessed: 13/04/11.

White House (2010a) *National Security Decision Directive Number 42 National Space Policy*, [Online] http://www.marshall.org/pdf/materials/845.pdf, Created: 21/04/10, Accessed: 25/09/12.

White House (2010b) *National Space Policy of the United States of America*, Washington D.C.: White House.

Wiedemann, C., H. Krag, J. Bendisch, H. Sdunnus (2004) ‘Analyzing costs of space debris mitigation methods’, *Advances in Space Research*, 34(5): 1241-1245.

Williams, A. J. (2010) ‘Flying the Flag: Pan American Airways and the Projection of US Power Across the Interwar Pacific’ in: F. MacDonald, R. Hughes and K. Dodds (eds.) *Observing States Geopolitics and Visual Culture*, I. B. Tauris & Co. Ltd.: 81-99.

Williams, A. J. (2011) ‘Reconceptualising spaces of the air: performing the multiple spatialities of UK military airspaces’, Transactions of the Institute of British Geographers, 36(2): 253-267.

Williamson, M. (2006) *Spacecraft Technology The early years*, London: The Institution of Engineering and Technology.

Williamson, R. A. (2012) ‘Assuring the sustainability of space activities’, *Space Policy*, 28(3): 154-160.

Wright, D. (2007) ‘Debris from China's Kinetic Energy ASAT Test’, [Online] http://www.ucsusa.org/global_security/space_weapons/debris-from-chinas-asat-test.html Accessed: 16/11/07.

Wright, D. (2009) ‘Colliding Satellites: Consequences and Implications’, [Online] http://www.ucsusa.org/assets/documents/nwgs/SatelliteCollision-2-12-09.pdf, Created: 26/02/09, Accessed: 25/10/10.

Wright, D., L. Grego and L. Gronlund (2005) *The Physics of Space Security A Reference Manual*, Cambridge, MA: American Academy of Arts and Sciences.

Wright, R. (1992) *Stolen Continents Conquest and Resistance in the Americas*, London: Phoenix Press.

Ziegler, D. W. (1999) ‘Safe Heavens: Military Strategy and Space Sanctuary’ in: B. M. DeBlois (ed.) *Beyond the Paths of Heaven The Emergence of Space Power Thought*, Maxwell Air Force Base, AL: Air University Press: 185-245.