The risk that Cyber-attacks pose to Outer Space Assets: How can international dialogue and cooperation help?

by

Mike D. Bilodeau

A thesis submitted to McGill University
in partial fulfilment of the requirements of
the degree of **MASTER OF LAWS (LL.M.)**

Institute of Air and Space Law
McGill University, Faculty of Law
Montreal, Quebec

December 2019

ACKNOWLEDGEMENTS

Firstly, I would like to thank New Zealand Defence, Universities New Zealand – Te pōkai tara, and the Freyberg Scholarship Selection Board for the opportunity to attend McGill University and the Institute of Air and Space Law. This once-in-a-lifetime opportunity, to pursue my passion under the tutelage of such a brilliant group of professors and alongside such a talented group of students, is one that I will forever be grateful for.

My thanks also goes out to my thesis supervisor, Professor Brian F. Havel, who has provided invaluable guidance throughout my LLM. journey. So too do I extend my appreciation to my fellow co-agents in the Manfred Lachs mooting competition – we came, we saw, and we won a couple of plaques.

Lastly, and most importantly, I would like to thank my family, and my partner Nicole. Were it not for your love and support, I would never have been able to achieve what I have and, for that, I will forever be grateful.

ABSTRACT

As the public and private sectors continue their rapid expansion into the outer space environment, both government and civil society witness their dependence on outer space assets permeating every facet of their day-to-day lives. While there has been a significant amount of dialogue surrounding the protection of such assets from deliberate attacks, this has tended to focus more on kinetic threats, such as anti-satellite weapons, and dual-use technologies. This focus, however, has diverted attention from what is a far more realizable and realistic threat – that of a cyber-attack being carried out on space assets. Not only do cyber-attacks have the demonstrated ability to physically incapacitate a space asset, but they can also be carried out with relatively minimal materials and without a particularly specialised set of skills – thus making them a significantly more attractive option to a potential attacker than their kinetic counterparts. What makes this even more worrisome is that this risk is gradually growing, and is doing so in an international policy lacuna. As such, the purpose of this thesis is to advise how international cooperation, dialogue and policy can better be leveraged to mitigate the risk that cyber-attacks pose to outer space assets.

The introduction to this thesis will provide an overview of this issue and the objectives, and will define some of the technical terminology which will be utilised throughout. Following from this, Part I will assess the threat which cyber-attacks pose to outer space assets, as extrapolated from previous attacks on such assets, as well as attacks on other critical pieces of national infrastructure. Part II will look at ground-level best practice guidelines, both in terms of industry, as well as domestic regulation. Part III will then review the existing initiatives in place to curb the risk that cyber-attacks pose to outer space assets at all levels of international engagement. Finally, Part IV will analyse how international engagement can be better utilised to mitigate this risk, drawing upon those measures considered most effective from the previous sections.

RÉSUMÉ

Alors que les secteurs public et privé poursuivent leur expansion rapide dans le domaine de l'espace extra-atmosphérique, les gouvernements et la société civile constatent leur dépendance à l'égard des technologies et biens spatiaux dans tous les aspects de leur vie quotidienne. Bien que les discussions sur la protection de ces biens contre les attaques soient nombreuses, elles se concentrent plutôt sur les menaces cinétiques telles que les armes antisatellites et les technologies à double usage. Cette approche a détourné l'attention d'une menace beaucoup plus réaliste et réalisable – celle d'une cyberattaque menée contre des biens situés dans l'espace. Non seulement les cyberattaques ont la capacité avérée de neutraliser physiquement un bien spatial, mais elles peuvent aussi être conduites avec un matériel relativement minimal et sans compétences particulièrement spécialisées – ce qui, pour un assaillant potentiel, en fait une option beaucoup plus attrayante que ses homologues cinétiques. Cette situation est rendue encore plus inquiétante par l'accroissement progressif du risque et, de surcroît, par une lacune de la politique internationale. L'objectif de cette mémoire est précisément d'indiquer comment mieux tirer parti de la coopération, du dialogue et des politiques internationales pour atténuer le risque que les cyberattaques posent aux biens spatiaux.

L'introduction de cette mémoire donnera un aperçu de cette question et de ses objectifs et définira certains termes techniques qui seront utilisés dans son développement. A cette suite, la partie I évaluera la menace que les cyberattaques font peser sur les biens spatiaux, telle qu'elle a été extrapolée des attaques antérieures contre ces biens comme d'autres éléments essentiels des infrastructures nationales. La partie II examinera, au niveau du sol, les lignes directrices sur les meilleures pratiques s'agissant tant de l'industrie que de la réglementation nationale. La partie III passera ensuite en revue les initiatives à tous les niveaux de la coopération internationale visant à réduire le risque que les cyberattaques posent aux biens

spatiaux. Enfin, la partie IV analysera comment cette coopération internationale peut être mieux utilisée pour atténuer ce risque, en s'appuyant sur les mesures jugées les plus efficaces dans les sections précédentes.

ACRONYMS AND ABBREVIATIONS

ACORN	Australian Cyber-crime Online Reporting Network
ACSC	Australian Cyber Security Centre
ANZPAA	Australia New Zealand Policing Advisory Agency
ARF	ASEAN regional forum
ASAT	Antisatellite Weapon
ASEAN	Association of Southeast Asian Nations
CARICOM	Caribbean Community
CCDCOE	Cooperative Cyber Defence Centre of Excellence
CECC	Council of Europe Convention on Cyber-crime
CD	Conference on Disarmament
CERT	Computer Emergency Response Team
CICTE	Inter-American Committee against Terrorism
CIRM	Cyber Insider Risk Mitigation
COPUOS	Committee on the Peaceful Uses of Outer Space
CSIRTs	Computer Security Incident Response Teams
CTU	Caribbean Telecommunications Union
DLR	Deutsches Zentrum für Luft (German Space Agency)
ECtHR	European Court of Human Rights
ESA	European Space Agency
EU	European Union
GGE	Group of Government Experts
GGE:DFICT	Group of Governmental Experts on Developments in the Field of Information and Communications Technologies in the Context of International Security
GGE:PAROS	Group of governmental experts on further practical measures for the prevention of an arms race in outer space
ICAO	International Civil Aviation Organization
ICJ	International Court of Justice
ICT	Information and Communications Technology
IHL	International Humanitarian Law
IT	Information Technology
ITU	International Telecommunication Union
NASA	National Aeronautics and Space Administration
NATO	North Atlantic Treaty Organization
NCS	National Cybersecurity Strategy
NSA	United States National Security Organization
OAS	Organization of American States
OECD	Organization for Economic Co-Operation and Development
OSCE	Organization for Security Co-operation in Europe
PAROS	Prevention of an Arms Race in Outer Space
PKI	Public Key Infrastructure
PNT	Positioning, Navigation and Timing
RF	Radio Frequency
SARP	Standards and Recommended Practices
SCO	Shanghai Cooperation Organization
SSGC	Secretariat Study Group on Cybersecurity
SSL	Secure Sockets Layer
TCBM	Transparency and Confidence Building Measures

UN	United Nations
UNODA	United Nations Office for Disarmament Affairs
UNODC	United Nations Office on Drugs and Crime
UNIDIR	United Nations Institute for Disarmament Research
WIPO	World Intellectual Property Organization

TABLE OF CONTENTS

INTRODUCTION

A. Issue and Objectives

Ever since the dawn of the cyber revolution, the international community has been wary of the dangers associated with cyber space.[1] Working hand-in-glove with this growing disquiet, the topic of cyber security has long been raised by a wide number of States[2] in a broad range of forums, be they focused on trade,[3] defence,[4] or policy.[5] Now, only eight decades since the first fully-functional digital computer was created,[6] we see the issue raised in regard to outer space assets.

In 2019, a Group of Governmental Experts (GGE:PAROS) comprising individuals from 26 different Member States, gathered in New York to consider and make recommendations on substantial elements of an international legally binding instrument for the prevention of an arms race in outer space.[7] As part of these discussions, the group discussed the variety of possible threats to outer space activities and, while the majority of such threats had been discussed for decades – anti-satellite weapons, dual-use technologies, nuclear detonations, and so forth – the pronounced newcomer to the room was cyber-attacks.[8]

---

[1] INTERPOL Third INTERPOL Symposium on International Fraud (Paris 11-13 December 1979)
[2] Concern about the threat that cyber-attacks pose to piece of national infrastructure has been expressed in a range of State papers, including those of New Zealand, as per New Zealand Ministry of Defence, Defence White Paper 2010 pp. 25, 41; the US, as per E Burger, G Bordacchini, Yearbook on Space Policy 2017 – Security in Outer Space: Rising Stakes for Civilian Space Programmes (Switzerland: Springer 2017) at 9; the UK, as per UNODC "United Kingdom National Cyber Security Strategy 2016 to 2021", accessed 06 June 2019, online: <https://sherloc.unodc.org/cld/treaties/strategies/united_kingdom/gbr0005s.html?lng=en&tmpl=sherloc>; and the EU, as per Steve Morgan "2019 Cybersecurity Almanac: 100 Facts, Figures, Predictions and Statistics" (06 Feb 2019, New York) online: <https://cybersecurityventures.com/cybersecurity-almanac-2019/>.
[3] Organisation for Economic Co-operation and Development, "Global Forum on Digital Security for Prosperity" (accessed 10 August 2019) online: <https://www.oecd.org/internet/global-forum-digital-security/about/>
[4] Institute for Defence and Government Advancement, "5th Annual Cyber Security for Defence" (accessed 10 August 2019) online: <https://www.idga.org/events-cybersecurityfordefence>
[5] USTelecom. "USTelecom Cybersecurity Policy Forum: National Cyber Policy Guidance", (accessed 10 August 2019) online: <https://www.idga.org/events-cybersecurityfordefence>
[6] The ENIAC computer was built in 1946, having taken 3 years to build, occupying 1800 square feet, utilizing 18000 vacuum tubes and weighing almost 50 tons, as per ComputerHope, "When was the first computer invented?" (Computer hope, February 2019) online: <http://www.computerhope.com>
[7] UNODA, Report by the Chair of the Group of governmental experts on further practical measures for the prevention of an arms race in outer space, (New York, 31 January 2019) online (pdf): <https://s3.amazonaws.com/unoda-web/wp-content/uploads/2019/02/oral-report-chair-gge-paros-2019-01-31.pdf>
[8] *Ibid* at 9.

The context of these discussions focused not only on the threat posed by cyber-attacks, but on what international regulation is in place to help mitigate this threat and to hold perpetrators of such attacks accountable. In this regard, the GGE:PAROS concluded that, while the most applicable multilateral regulatory instrument is the *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies* (Outer Space Treaty),[9] this lacks the definitive prohibitions required to protect such assets.[10] The Outer Space Treaty, while expressing a desire for States to utilize outer space and its celestial bodies for 'peaceful purposes', offers very little in terms of clarification of what these peaceful purposes entail, and what actions can be taken if these purposes are not abided by.[11]

While not explicitly discussed by the GGE:PAROS, one may also be surprised by the relative lack of binding international policy in regards to cyber-attacks. In the context of cyber space, the most relevant multilateral regulatory instrument is the *Budapest Convention on Cyber-crime*,[12] which is notably the first and only binding cyber-crime multi-lateral instrument in force today. However, this has some significant limitations, with many considering that this is a criminal justice treaty and that it does not, in fact, cover State actors.[13] Furthermore, there is a concern surrounding the membership of this Treaty, in that it does not include key States of interest, including India, China and Russia. In light of this lack of any clear international *lex specialis* regulating undesirable cyber acts, States have found it difficult to pinpoint exactly on

[9] Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, 27 January 1967, 610 UNTS 205 (entered into force 10 October 1967) at preamble and art IV [Outer Space Treaty].
[10] UNODA, *supra* note 7 at 6-8
[11] Outer Space Treaty, at preamble and art IV.
[12] Convention on Cyber-crime (European Treaty Series No. 185, Budapest, 23.XI.2001) online: <https://www.coe.int/en/web/conventions/search-on-treaties/-/conventions/rms/0900001680081561> [Budapest Convention]
[13] A Seger, "India and the Budapest Convention: Why not?" (ORF Foundation, Oct 20, 2016) online: <https://www.orfonline.org/expert-speak/india-and-the-budapest-convention-why-not/>

what basis cyber-attacks which occur over State lines can be considered illegal.[14] This was demonstrated in 2012, when a large number of cyber-attacks, originating from China, were launched against American entities,[15] after which US lawyers and academics were unable to conclusively find legal grounds to demonstrate that such actions were unlawful under international law.[16] Such circumstances have led to rather broad-reaching interpretations of existing international regulation, with some pointing to the 'use of force' prohibition outlined in Article 2(4) of the UN Charter[17] as a potentially guiding mandate.[18]

The aim of this thesis then, is to determine what law, if any, is currently in place to protect a wide-ranging array of space assets[19] from cyber-attacks arising outside the victim's State and, following from this, to determine how international law, policy, and cooperation can be better deployed to serve this purpose. This is particularly important as, given that software lies at the heart of all complex space-based systems, both space-based and ground-based space-components are vulnerable to cyber-attacks.[20] Additionally, as a result of the emerging "cyber physical connection" cyber-attacksare now capable of leading to the physical destruction of

[14] Such has been the case in numerous cyber-attacks to other pieces of infrastructure; as per Tzeng, "The State's Right to Property Under International Law" (Yale Law Journal, Vol. 125, Issue 6, 2016) 1548-1819, online: <https://www.yalelawjournal.org/comment/the-states-right-to-property-under-international-law>

[15] Ellen Nakashima, Confidential Report Lists U.S. Weapons System Designs Compromised by Chinese Cyberspies, (Washington Post May 27, 2013) online: <http://www.washingtonpost.com/world/national-security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html>; US, Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2015, Off. Secretary Def. 38-39 (Apr. 7, 2015) online
(pdf): <http://www.defence.gov/Portals/1/Documents/pubs/2015_China_Military_Power_Report.pdf>.

[16] Tzeng, *supra* note 14.

[17] Charter of the United Nations, Oct. 24, 1945, 1 U.N.T.S. XVI [UN Charter]; Schmitt, Michael N. et al. Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare, Michael Schmitt & Liis Vihul, eds, (Cambridge: Cambridge University Press, 2017) [Tallinn Manual 2.0].
at 48-51.

[18] Tzeng, *supra* note 14.

[19] Such assets play a fundamental role in our defence systems, connectivity, our ability to predict and contain natural disasters, and our economic trade, as per D Livingston, P Lewis Space, the Final Frontier for Cyber Security? (Chatham House, The Royal Institute of International Affairs, September 2016) at ii

[20] C Johnson, University of Glasgow "Cyber Security for Space Based Systems" <www.gla.ac.uk>

equipment (and subsequently the loss of mission and loss of life)[21] and, what is perhaps most worrisome, is that such attacks are also becoming increasingly affordable and easy to execute.[22]

To address these issues, Part I of this thesis will look at the threats which cyber-attacks pose to outer space assets, providing a comprehensive overview of cyber-attacks on both outer space assets and other key pieces of national infrastructure. This Part will also explore those actors who may seek to perpetrate such cyber-attacks against outer space assets, since the origin of attacks helps to determine the resources and threat-level that lie behind them.

Part II will look at ground-level best practices which are currently implemented within States to combat and discourage cyber threats, both at an industry and a domestic regulation level. It is important to analyse these practices and regulatory regimes in both well-established and newly space faring nations, as this helps to determine the viability of options at an international level, and also determines the amount of capacity building and assistance that may be available from (or required by) States. While States scattered through all regions of the world now have cyber security regimes in place,[23] the lack of international consensus on the structure of these has meant that the security of key pieces of national infrastructure from cyber based attacks, and the accountability faced by those who initiate such attacks, remains uncertain.[24] It is this lack of certainty and lack of consensus which drives the focus of this thesis, considering the international *lex lata* and *lex ferenda*[25] relating to cyber-attacks to outer space assets, and thus brings us to Parts III and IV.

---

[21] N Weiss "UNIDIR Space Security Conference 2017 Celebrating the Outer Space Treaty: 50 Years of Space Governance and Stability Conference Report" at 15 (20-21 April, 2017) <http://www.unidir.org/files/publications/pdfs/unidir-space-security-2017-en-685.pdf>

[22] C Baylon, R Brunt, D Livingstone Cyber Security at Civil Nuclear Facilities: Understanding the Risks (Chatham House Report, September 2015) at 3

[23] J Lewis, G Neuneck, The Cyber Index: International Security Trends and Realities at 2 (New York and Geneva: United Nations Institute for Disarmament Research, 2013) online (pdf): <http://www.unidir.org/files/publications/pdfs/cyber index-2013-en-463.pdf>

[24] United Nations Office on Drugs and Crime, Comprehensive Study on Cyber-crime - Draft (UNODC, February 2013) at xx, online (pdf): <https://www.icao.int/cybersecurity/SiteAssets/UNODC/CYBER-CRIME_STUDY_210213.pdf> [UNODC Study on Cybercrime]

[25] *Lex Lata* roughly translates to 'the law as it is'. This is often contrasted with *lex ferenda*, which roughly translates to 'the law is it should be'.

Part III will focus on how existing international law, at a bilateral, regional, and multilateral level, may respond to a State-to-State cyber-attack against an outer space asset. In addition to focusing on *lex specialis*[26] for both outer space law and cyber law, this Part will also examine the *lex generalis* originating from foundational documents such as the United Nations (UN) Charter.[27]

Finally, Part IV will consider how international policy and cooperation can better be leveraged to mitigate the risks that cyber-attacks pose to outer space assets, summarizing what key criteria need be borne in mind to engage effectively in State-to-State dialogue to protect such assets. To meet this objective, the thesis will draw upon those measures considered in the prior discussion.

Cyber threats are a tremendous concern to States, representing a new era of warfare, where the very foundations of State dominance, on land, in the air, at sea, or in space, can be usurped by an emerging, artificial, and unconquerable domain; that of cyber space.[28] Such is the extent of this threat that now virtually all of the world's largest economies (including Russia, the US, the United Kingdom, China, France, the EU, and India) have publicly expressed concern about the threats posed by the build-up of cyber tools for military purposes, terrorist misuse of the internet, cyber-crime, and the disruption of critical infrastructure using cyber tools.[29] These concerns are well founded too, as cyber operations have already appeared

---

[26] The principle of *lex specialis derogate legi generali* means that a more specific.
law governing a particular legal issue takes precedence over a more general law, see Lachs, Manfred. The Law of Outer Space: An Experience in Contemporary Law-Making, Tanja Masson-Zwaan & Stephan Hobe, eds, (Leiden: Martinus Nijhoff, 2010) at 114; see also Hugo Grotius, De Jure Belli Ac Pacis. Libri Tres, Book II (1625) ¶XXIX which asserts, "What rules ought to be observed in such cases [i.e. where parts of a document are in conflict]. Among agreements which are equal…that should be given preference which is most specific and approaches most nearly to the subject in hand, for special provisions are ordinarily more effective than those that are general."

[27] UN Charter, *supra* note 17.

[28] The reason for this being that, while State entities have greater resources to dedicate to cyber defences etc, their strong dependence on complex cyber systems for support of military and economic activities creates new vulnerabilities, and these can be exploited by both State and non-state actors, as per J Nye Jr Nuclear Lessons for Cyber Security? (Strategic Studies Quarterly 5(4): 18-38, Winter 2011) at 20.

[29] Global Commission on the Stability of Cyber Space, "BRIEFINGS FROM THE RESEARCH ADVISORY GROUP" at 11, (New Delhi, November, 2017) online (pdf): <https://cyberstability.org/wp-content/uploads/2017/12/GCSC-Briefings-from-the-Research-Advisory-Group_New-Delhi-2017.pdf>

on the battlefield[30] and have done so only to find that this cyber technology has, as is so often the case, outpaced the law.[31] Before we progress further, however, it is important to delineate the scope and limitations of this thesis.

B. Scope and Limitations

Before launching into the substantive portion of this thesis, it is important to discuss the scope of the project. First and foremost, while this analysis will be looking at both industry-level and domestic practices to mitigate the risks of cyber-attacks, it does so exclusively for the purposes of pinpointing effective practices and determining the feasibility of international regulatory proposals, and will not seek to advance new industry standards or domestic regulation.

Secondly, this thesis will be focusing exclusively on attacks which are deliberately carried out against outer space assets. It will not be discussing cyber-attacks which simply utilize space assets, nor will it be discussing safety issues associated with unintentional malfunction of cyber dependent technology.

Thirdly, as cyber security in outer space assets is a relatively niche concern, this analysis will focus at times, both in its analysis and in its summation, on the wider aspects of cyber security.

Fourthly, while this thesis will be considering those criteria which should be borne in mind when considering a new international instrument, it will not be proposing articles or language which should be included in such an instrument – merely providing a range of initiatives which have been shown to work in the past, and discussing the advantages and disadvantages to their inclusion in any new Agreement.

---

[30] E Burger, G Bordacchini, *supra* note 2 at 9.
[31] Schmitt et. Al. "The Law of Cyber Targeting" at 20 (CCDCOE, Tallinn Paper No. 7, 2015) online (pdf): <https://ccdcoe.org/uploads/2018/10/TP_07_2015.pdf>

Lastly, while it may be tempting to apply the law of the sea to issues of outer space, given that both environments are regarded as *terra nullius*, this thesis will not seek to do so. As the esteemed Professor Bin Cheng has stated, the rules relating to outer space share basic legal condition of the high seas, "without, however, the special rules that pertain solely to the high seas."[32] As the United Nations Convention on the Law of the Sea already extensively covers the protection of flag-State ships[33] (while outer space asset protection has been discussed in various fora but never conclusively agreed upon) these competing *lex specialis* which flow from very different legal histories cannot be reconciled.

Considering the limitations encountered when writing this project, it is important to note that there is a severe underreporting of cyber incidents. Whether due to fears of reputational damage, security concerns, a lack of awareness of victimization and of reporting mechanism, or simply an impression that no benefit arises from making law enforcement aware of any such attacks, both private and State organizations have reported only a small fraction of total attacks to appropriate authorities.[34] This, compounded with the inability to accumulate cross-national comparative statistics due to the difficulties in consistently defining and identifying cyber-crime,[35] as well as the fact that police-recorded cyber-crime rates are dependent on levels of country development and specialised police capacity (as opposed to underlying crime rates),[36] means that the true extent of the threat which cyber-attacks pose may be drastically underestimated. Not only does this present some clear difficulties from a research perspective, from a practical standpoint it can also lead to severe underappreciation of the threat by organizations and (by proxy) significant underspending on cyber security.

---

[32] Bin Cheng, Studies in International Space Law at 638 (Oxford Scholarship Online, 2012) (1997)
[33] United Nations Convention on the Law of the Sea, Dec. 10 1982, 21 U.N.T.S. 1833, Subsection A
[34] As an example, the FBI's Internet Crime Complaint Center (IC3) stated that the number of reported cyber-crimes in the agency's reports only represent 10 to 12 percent of the total number actually committed in the U.S. each year; as per Internet Crime Complaint Center, 2016 Internet Crime Report at 5 (Federal Bureau of Investigation, 2016) online (pdf): <https://pdf.ic3.gov/2016_IC3Report.pdf>
[35] UNODC Study on Cybercrime, *supra* note 24 at 6.
[36] *Ibid* at xviii.

C. Technical Infrastructure and Terminology

Because this project considers two relatively specialised areas – outer space and cyber technologies – it is important to first provide a brief overview of some of the terminology which will be referred to throughout the study.

1. Key elements of outer-space infrastructure

Generally, outer-space infrastructure is separated into three primary segments – the space segment, the user segment, and the ground segment.[37] The 'space segment' consists of orbiting satellites which, for the purposes of this thesis are also referred to as the 'outer space assets' we are seeking to shield from attack. In multilateral agreements, these would be considered to be 'space objects'[38] (while the full extent of this term is oft-debated, the nuances of this nomenclature are not relevant for the purposes of this current debate, as the assets in this analysis would undoubtedly qualify as such).[39]

The 'user segment' consists of the equipment which utilizes the capabilities provided by the onboard satellite payloads (i.e. the user-terminals, in the case of communication satellites). While it is possible to 'steal' services and cause interruptions to the user segment through cyber-attack, this will not be regarded as an attack against an outer space asset, and thus will be excluded from the scope of this analysis.

Lastly, the 'ground segment', also referred to as the 'control segment', comprises a primary ground station (which monitors and controls the satellites), as well as secondary stations (which are connected to the primary station via communication link, and serve as a backup in case of failure in the primary station). Communication between the control room and

---

[37] Y Lipkin, A Shlomo, A Paz, D Menaker, G Mizrahi, N David Critical Infrastructure and Operational Technology Security, at 34 (Cyber Security Review, Delta Business Media, Autumn 2015)

[38] See, for example: Convention on International Liability for Damage Caused by Space Objects, Mar. 29, 1972, 24 U.S.T. 2389, 961 U.N.T.S. 187, art. I(d) and III [Liability Convention].

[39] The term 'object' as it relates to space activities has been interpreted by Professor Bin Cheng to include satellites, spacecraft, space vehicles, equipment, facilities, stations, installations and other constructions including their components. See: Bin Cheng, International Responsibility and Liability for Launching Activities, XX Annals of Air and Space Law 297 (1995), 297.

the satellites (uplink commands, as well as downlink telemetry from the satellite) are transmitted and received through base-band equipment and Radio Frequency (RF) equipment.[40] Given the ground segment's accessibility, its wide use of 'off-the-shelf' commercial IT components (both hardware and software)[41] and, perhaps counterintuitively, the fact that it is often not completely isolated from network systems, often requiring the same internet capabilities as any organization[42] (meaning that access to this segment is similar to hacking any terrestrial network, with various levels of security depending on the mission), it is this segment which is the most prone to cyber-attack,[43] potentially allowing an intruder to gain control of a satellite.

2. Key elements of cyber security

While the nuances of basic computer terms (such as 'computer', 'cyber space' etc.) have not been conclusively defined, these are intuitively understood well enough that they need not be discussed here. What are not particularly well-known, however, are the threats and security measures present in cyber space.

The earliest and perhaps most common computer-based misconduct is the act of 'phishing', which involves sending emails from a fraudulent account for the purposes of inducing a person to reveal personal information such as passwords. Since this early and relatively unsophisticated origin though, cyber-crime has evolved to include computer manipulation, computer forgery, damage to or modifications of computer data or programs,

[40] Y Lipkin, *supra* note 37 at 34.
[41] *Ibid* at 33.
[42] As an example, even satellites from several U.S. government space programs utilize commercially operated satellite ground stations outside the United States, some of which rely on the public Internet for ''data access and file transfers,'' according to a 2008 National Aeronautics and Space Administration quarterly report. See: US Government, 2011 Report to Congress of the US-China Economic and Security Review Commission, at 215 (112 Congress, First Session, November 2011) online (pdf): <https://www.uscc.gov/sites/default/files/annual_reports/annual_report_full_11.pdf>
[43] Y Lipkin, *supra* note 37 at 36.

unauthorised access to computer systems and service, and unauthorised reproduction of legally protected computer programs.[44]

Many of these acts are carried out utilizing technically complex 'malware',[45] which is a software specifically designed to disrupt, damage, or gain unauthorised access to a computer system, and requires significant technical skill to develop. Generally, such malware involves delivering malicious software in an unexpected format, such as word documents or PDF files, and includes so-called 'computer worms'[46] (self-replicating pieces of malware), 'zero-day malware' (intentionally or unintentionally built-in vulnerabilities into off-the-shelf hardware or software),[47] and 'spy-ware', which is a software which 'spies' on a computer, allowing an attacker to capture information like web browsing habits, e-mail messages, usernames and passwords (which can later be used to gain access to a system).[48]

Coming to cyber security, this is a broad term which generally includes all tools, policies, guidelines, training, best practices, and technologies which can be used to protect the wider cyber environment, as well as organizations' and users' assets.[49]

3. Summary

While the international community has long realized the cross-border threat of cyber-attacks, these borders have only recently expanded into a new environment: outer space. These environments of cyber space and outer space are both highly technical and almost universally utilized, with their uses evolving at an astounding rate. With every step of evolution, however,

---

[44] United Nations, "UN Manual on the Prevention and Control of Computer Related Crime" (United Nations, 1994) online (pdf): <http://216.55.97.163/wp-content/themes/bcb/bdf/int_regulations/un/CompCrims_UN_Guide.pdf>

[45] As mentioned above however, while these means are quite technically complicated to develop, these items can now be purchased online, thus meaning that skill levels of the attacker are not necessarily indicative of the level of harm they can cause. As per UNODC Study on Cybercrime, *supra* note 24 at 42-43.

[46] Conti, Dargahi, Dehghantanha "Cyber threat Intelligence: Challenges and Opportunities" (Springer Publishing, 2018) at 2.

[47] M Azriel "Emergence of Cyber Security Products for Space Systems" (October 5, 2012) online: <www.spacesafetymagazine.com>

[48] *Ibid*.

[49] International Air Transport Association, Cyber Security Fact Sheet (IATA, December 2018) at 1, online (pdf): <https://www.iata.org/pressroom/facts_figures/fact_sheets/Documents/fact-sheet-cyber security.pdf>

we see new risks arise, as mankind's dependence on outer space assets and cyber connectivity (and, in these circumstances, the interplay between the two) provides a crucial linchpin for modern day society. The next Part of this thesis then, will provide a risk-analysis, outlining the extent of the threat that cyber-attacks pose to outer space assets.

PART I

THE THREAT THAT CYBER-ATTACKS POSE TO OUTER SPACE ASSETS

Before States determine what resources should be dedicated to any threat, they must first determine the *extent* of the threat. In this Part, we will first look at the risk that cyber-attacks pose in general, and then review instances where key pieces of national infrastructure have been victims of cyber-attacks in the past. Following from this, we will look at which actors may seek to perpetrate such an attack, as this helps to predict the potential targets and resources behind an attack, thereby building a fuller picture of the risks which States face.

A. Cyber-attacks – an ever-growing and evolving threat

As both the general public and States become exponentially more connected by (and dependent on) the services which the internet provides,[50] the frequency of cyber-crime has also been increasing at a rapid rate.[51] This increase in frequency has also meant that hacking tools and kits for cyber-attacks, identity theft, malware, ransomware, and other nefarious purposes are becoming more accessible and affordable to any person wishing to carry out an attack (with many attack tools available for a modest price, or downloaded for free from the internet),[52]

[50] UNODC Study on Cybercrime, *supra* note 24 at xvii.
[51] A UNODC report which asked participating countries about cyber-crime trends in their own country over the past five years reported that all reporting law enforcement officials in 18 countries in Africa and the Americas responded that cyber-crime was either increasing or strongly increasing. See UNODC Study on Cybercrime, *supra* note 24 at 7.
[52] S Morgan, *supra* note 2.

originating from a wider range of sources,[53] and evolving to be more damaging every day.[54] Additionally, and potentially most importantly, these attacks are low risk, allowing attackers to evade detection by hiding their tracks through both technical means, and by exploiting gaps in domestic and legal regimes.[55]

States have dedicated significant resources to combatting this threat in terms of their outer space assets, with the US NASA program making significant budget allocations for cyber security,[56] China's military strategy outlining that "outer space and cyber space have become new commanding heights in strategic competition among all parties",[57] and the European Space Agency (ESA) going so far as to launch its own cybersecurity excellence centre.[58] Outside of outer-space assets specifically, a significant number of States, including Russia, China, the United States, the UK, France, the EU, and India, all state in their cyber strategies that the disruption of critical infrastructure is a significant concern.[59]

1. A history of cyber-attacks

To understand the risk which cyber-attacks pose to outer space assets, it is useful to examine how such attacks have affected national infrastructure in the past. Given that cyber-attacks on outer space assets are a recent concern with a relatively limited number of reported occurrences, in addition to looking at space assets specifically, this thesis will look toward other infrastructure areas, including aviation and electricity networks.

---

[53] A public release by two internet security companies, Akamai and Symantec, shows that malicious computer programs now originate in more than 190 countries. See Akamai, "State of the Internet Report," March 2008 online (pdf): <https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/akamai-q1-2008-state-of-the-internet-connectivity-report.pdf>

[54] Government of Canada "Canada's Cyber Security Strategy: For a stronger and more prosperous Canada" at 6 (2010) online (pdf): <https://sherloc.unodc.org/res/cld/treaties/strategies/canada/can0003s_html/Canadas_Cyber_Security_Strategy_ENG.pdf>

[55] *Ibid* at 4-5.

[56] Smith, Marcia. "NASA's FY2020 Budget Request" (13 June 2019) online: <https://spacepolicyonline.com/fact-sheets-reports/>

[57] E Burger, G Bordacchini, *supra* note 2 at 102

[58] *Ibid* at 209.

[59] Global Commission on the Stability of Cyber Space, *supra* note 29 at 34.

a) Outer Space Assets

While reported instances of cyber-attacks against outer space assets are rare, there have been some notable occurrences, most often resulting from the transfer of 'conventional' viruses (typically from USB sticks) to mass-market operating systems (e.g. Linux) carried out at the ground segment during periodic updates.[60]

Examples of when such attacks occurred were provided in a 2011 US-China Economic and Security Review Commission Report, which outlined several instances where US government satellites experienced interference consistent with a cyber-attack:[61]

i. In perhaps the first and most notable attack on outer space assets, in 1998 the German-US ROSAT space telescope inexplicably turned toward the sun, damaging a critical optical sensor and rendering the telescope useless. After analysis, NASA investigators determined that the accident was linked to a cyber intrusion at the Goddard Space Flight Centre;[62]

ii. In 2008, NASA experienced two short events of disrupted control over the earth observation satellite Terra/EOS AM-1 (lasting two minutes in June and nine minutes in October). In both cases, the attack achieved all steps required to command the satellite, though the attackers did not issue those commands;[63]

iii. In 2008 two separate events affected the satellite Landsat-7. Both cases were suspected of originating through a compromised ground station in Norway and lasted for approximately 12 minutes each.[64]

[60] C Johnson, *supra* note *22*.
[61] US Government, *supra* note 42, at 216.
[62] Y Lipkin, *supra* note 37 at 33
[63] US Government, *supra* note 42 at 216.
[64] *Ibid.*

These examples are important as they demonstrate the vulnerability of space assets to cyber-attacks, as well as the potentially mission-critical damage which can occur when such an attack takes place.

b) Aviation

The crossover between aviation and outer space is perhaps more prominent than many may assume. With advancements in technology pushing the aviation and space environments ever closer together,[65] and both growing more dependent on ground-based remote control by cyber means,[66] these environments are quickly finding themselves utilizing similar technologies, which are subject to similar risks.

Whereas damaging attacks on actual aircraft may not have taken place (though there has been speculation about whether the crash of Spanair flight 5022 at Barajas airport in 2008 was due to malware),[67] numerous confirmed cyber-attacks have taken place in other critical areas of the civil aviation sector. Even within the last twelve months at the time of writing, British Airways was subject to a cyber-attack which placed the information of more than 250,000 customers at risk,[68] Cathay Pacific had its computer system compromised for seven months, potentially exposing the personal information and travel histories of up to 9.4 million people,[69] and Bristol Airport was subject to a ransomware attack which led to the failure of its

[65] See Jeff Foust, Blue Origin plans to start selling suborbital spaceflight tickets next year (Spacenews, 21 June 2018) online: <https://spacenews.com/blue-origin-plans-to-start-selling-suborbital-spaceflight-tickets-next-year/> and FAI, Statement about the Karman line (FAI, November 2018) online: <https://www.fai.org/news/statement-about-karman-line>

[66] ICAO "Civil Aviation Cybersecurity Information Repository", online: <https://www.icao.int/cybersecurity/Pages/default.aspx>

[67] Leslie Meredith, Malware implicated in fatal Spanair plane crash (NBCNews, 20 August 2010) online: <http://www.nbcnews.com/id/38790670/ns/technology_and_science-security/t/malware-implicated-fatal-spanair-plane-crash/#.XLemyOi6O70>

[68] Charlie Osbourne, British Airways: Cyberattack, data theft bigger than we first thought (ZDNet, October 25 2018) online: <https://www.zdnet.com/article/british-airways-cyberattack-data-theft-bigger-than-we-first-thought/>

[69] Raymond Zhong, Cathay Pacific Data Breach Exposes 9.4 Million Passengers (New York Times, 25 Oct 2018) online: <https://www.nytimes.com/2018/10/25/business/cathay-pacific-hack.html>

display screens for two days.[70] Such is the ever-present danger of this risk that, at a recent Air Transport IT Summit, experts stated that it is not a question of whether a particular carrier will be attacked, but instead, a question of when.[71] Given the extent of these threats (and particularly, the concern attached to this threat by industry) cyber security policy in aviation has progressed perhaps further than any other industry.[72]

Given the concern which the aviation industry places on cyber-attacks, aviation security policy has developed significantly, thus making it a useful environment for policy inspiration. While it does fall outside of the scope of this thesis, it could be a useful avenue of further study to analyse how the raft of international aviation security instruments have helped to address problems associated with unlawful interference, such as through their creation of international offences and the establishment of almost universal jurisdiction over such offences.

c) Electricity networks

While electricity distribution networks are clearly distinguishable from outer space and aviation assets, they are among States' most critical pieces of national infrastructure, and thus may find themselves prime targets for cyber-attacks.

The most prominent instance of a disruptive cyber-attack against an electricity network was perpetrated against the Ukrainian electricity distribution companies Prykarpattya Oblenergo and Kyiv Oblenergo, which were attacked on 23 December 2015, disrupting over 50 substations of the distribution networks, and affecting 220'000 consumers.[73] This particular incident was so destructive that it was incorporated explicitly into the UK's cyber defence

[70] BBC, Cyber-attack led to Bristol Airport Blank Screens (16 Sep, 2018) online: <https://www.bbc.com/news/uk-england-bristol-45539841>
[71] Fox, L., Cyber security moves up the airline agenda as threats are no longer an if. (TNooz, 4 July 2016) online: <https://www.tnooz.com/article/cyber security-airlines-sita-it-trends/>
[72] PriceWaterhouseCoopers, 2015 Global airline CEO survey, Getting clear of the clouds: Will the upward trajectory continue? (PWC, Dec. 2015) at 4, online (pdf): <http://www.pwc.com/us/en/industrial-products/publications/assets/pwc_2015_global_airline_ceo_survey.pdf>
[73] E Burger, G Bordacchini, *supra* note 2 at 10.

strategies, directing their defence focus towards developing good security practices across their critical national infrastructure.[74]

d) Other attacks against a State's assets

2008 was a particularly notable year in terms of cyberwarfare, in that it was here that cyber activities first played a major part in international conflicts. During the Georgian-Russian conflict, both State and civilian cyber-attacks were launched alongside kinetic military operations, playing a significant role in the conflict.[75] Since this time, we have seen cyber-attacks featuring in a number of conflicts.[76]

Perhaps the most notable cyber-attack against State assets was the 2010 'Stuxnet' attacks, where a 'weaponised' malware ('weaponised' in that it was directed at a specific target)[77] was introduced to Iran's nuclear program via a flash drive,[78] causing the facility's centrifuges to speed up or down in such a way that they destroyed themselves, all while leaving normal indicators on computer readings. [79] This is an extremely important example as it fully demonstrates the critical physical damage that can result from a cyber-attack in modern systems. Additionally, due to the complexity of this attack, some have argued that such attacks lie well beyond the normal risk analysis, thus prompting a change in standard risk assessment protocols.[80] It has been posited by some academics that the Stuxnet malware attack accounts for the first instance of "armed attack" in terms of international law.[81]

---

[74] HM Government "NATIONAL CYBER SECURITY STRATEGY 2016-2021" at 21 (2016) online (pdf): <https://sherloc.unodc.org/res/cld/treaties/strategies/united_kingdom/gbr0005s_html/National_Cyber_Security_Strategy_2016_to_2021_English.pdf>
[75] M Schmitt, *supra* note 31 at 1.
[76] E Burger, G Bordacchini, *supra* note 2 at 9
[77] Computer Weekly "Stuxnet: A wake-up call for nuclear cyber security attacks" W Ashford (21 October 2015) <www.computerweekly.com>
[78] C Baylon, *supra* note 22 at 12.
[79] E Burger, G Bordacchini, *supra* note 2 at 10
[80] Computer Weekly, *supra* note *77*.
[81] Global Commission on the Stability of Cyber Space, *supra* note 29 at 85.

e) Summary

By analysing this history of cyber-attacks against critical assets, we see how such attacks are at the forefront of States' minds in offence and defence in conflict scenarios. As it relates to outer space assets, this is of particular concern, given that such assets are used for a wide variety of State services such as communication, air transport, maritime trade, financial services, environmental monitoring, and military offence and defence systems (the US, Russia, China and India, all of which can be considered space-faring superpowers, have dedicated satellites for both military communication and imagery,[82] and rely on satellites for monitoring, PNT, reconnaissance, and guidance).[83] This increases the chances that these assets will be targeted, particularly in instances of warfare.

2. Potential perpetrators

In order to understand the extent of the threat which outer space assets face, it is important to look at who may be seeking to perpetrate such an attack. This helps to predict the method of attack, the resources behind such an attack, and the degree of malice which comes with such attacks.

a) Individual hackers

Starting with the lowest risked offender (in terms of abilities, resources and motives), we have traditional hackers. These individuals tend to develop their skills and commit their attacks for 'bragging rights', generally not focusing on a specific target, but instead seeking out vulnerabilities in systems. Defences at this level can generally be limited to establishing a perimeter around an organisation's information system infrastructure, and defending that perimeter using firewalls, antivirus programs, and other commercially available tools.[84]

---

[82] Union of Concerned Scientists, "UCS Satellite Database" online: <https://www.ucsusa.org/>
[83] D Livingston, P Lewis, *supra* note 19 at ii.
[84] Civil Air Navigation Services Organisation, CANSO Cyber Security and Risk Assessment Guide (CANSO, June 2014) at 5, online (pdf): <htttps://www.canso.org/sites/default/files/CANSO%20Cyber%20Security%20and%20Risk%20Assessment%20Guide.pdf>

b) Criminal organization

According to a study by the United Nations Office on Drugs and Crime (UNODC), upwards of 80 per cent of cyber-crime acts originate from some form of organised activity, with cyber-crime black markets established on a cycle of malware creation, computer infection, botnet management, harvesting of personal and financial data, data sale, and 'cashing out' of financial information.[85] While clearly this brand of threat tends to focus around theft of data for financial gain, there is an ongoing concern that there is a range of cyber expertise in the criminal world which is available to the highest bidder.[86]

To combat this level of threat, focus must be directed at protecting information and systems, not just at the perimeter but wherever it resides within the enterprise, using techniques such as hard drive encryption.[87]

c) Terrorists

The relatively recent rise of so-called 'catastrophic terrorism' (that is, terrorism which pursues not political change but instead, unlimited goals and global impact)[88] as well as the high sophistication and extreme wealth of certain terrorist organizations,[89] means that the risk of a sophisticated cyber-attack by a terrorist organization is a significant concern. Terrorist cells have already been known to utilize the internet to support their recruitment, fundraising and propaganda activities, and are notably aware of the potential for using the western world's dependence on cyber systems as a vulnerability to be exploited.[90] Though their capability to

[85] UNODC Study on Cybercrime, *supra* note 24 at 39.
[85] *Ibid*.
[86] Government of Canada, *supra* note 54 at 5.
[87] CANSO, *supra* note 84 at 5.
[88] A Arbatov, A Pikaev and V Dvorkin Nuclear Terrorism: Political, Legal, Strategic and Technological Aspects (Russian Politics and Law, Vol 46, No 1, Jan-Feb 2008) at 58.
[89] L Napoleoni Modern Jihad: Tracing the Dollars Behind the Terror Networks (Pluto Press, London, 2003) at 203-206.
[90] Government of Canada, *supra* note 54 at 5.

commit a seriously damaging cyber-attack is debated,[91] a number of terrorist groups, including Al-Qaeda, have expressed their intention to launch cyber-attacks against Western states.[92]

The United Kingdom has notably expressed concern that, as an increasingly computer-literate generation engages in extremism, the number of skilled extremist lone actors will increase, as will the chances that a terrorist organisation will enlist established insiders to achieve their goals.[93] This concern has been shared by a number of States, including China, the United States, Russia,[94] France, the EU, and India, all stating in their cyber related strategies that terrorists' use of the internet is a significant concern.[95] Given the potential implications of an attack against an outer space asset, an attack against such an asset could potentially be a natural extension of terrorism.

Defence at this level requires continuous internal monitoring and system hardening throughout the enterprise.[96] In this regard, it is also important to note that cyber security can not be considered a 'one and done' exercise, but instead requires constant innovation and monitoring to ensure early detection of intrusions.[97] This type of constant innovation is particularly important given that when attacks are carried out by sophisticated hackers, they will often occur over a long period (6-18 months), allowing the hackers the opportunity to identify critical systems, locate valuable data, and execute devastating attacks.[98]

In line with this, organizations can utilize 'penetration testing' to bolster defences, wherein cyber security professionals utilize the same techniques used by criminal hackers (such

[91] HM Government, *supra* note *77* at 19.
[92] Government of Canada, *supra* note 54 at 5.
[93] HM Government, *supra* note *77* at 19.
[94] CCDCOE, "Basic Principles for State Policy of the Russian Federation in the Field of International Information Security to 2020," online (pdf): <https://ccdcoe.org/sites/default/files/strategy/RU_state-policy.pdf>
[95] Global Commission on the Stability of Cyber Space, *supra* note 29 at 34.
[96] CANSO, *supra* note 84 at 5.
[97] PriceWaterhouseCoopers, Aviation perspectives 2016 special report series: Cybersecurity and the airline industry – Part 1 of 4: Introduction (PWC, 2016) at [3], online (pdf): <https://www.pwc.com/us/en/industrial-products/publications/assets/pwc-airline-industry-perspectives-cybersecurity.pdf>
[98] PriceWaterhouseCoopers, Aviation perspectives: 2016 special report series: Cybersecurity and the airline industry – part 3 of 4: detection (PWC, 2016) at [3], online (pdf): <https://www.pwc.com/us/en/industrial-products/publications/assets/pwc-airline-industry-perspectives-cybersecurity-detection.pdf>

as password cracking, code injection, and phishing) to check for potential vulnerabilities and areas of weakness.[99]

d) States

Given the key role that outer space assets play in advancing political, economic, commercial and military objectives,[100] it stands to reason that a rival State could be the most likely candidate to commit an attack on a State's outer space assets.

Indeed, State-to-State cyber-attacks are now becoming commonplace in both offensive and defensive stratagems of States.[101] Authoritative Chinese military writings[102] have advocated for cyber-attacks against control systems, particularly as they relate to satellite control facilities.[103] So too has the US shown its willingness to utilize cyber-attacks, with President Barack Obama notably ordering the Pentagon to increase its cyber strikes against North Korea's missile programme[104] and encouraging ongoing digital incursions into Russia's electric power grid.[105] The extent of this threat is far-reaching too, with 12 of the 15 largest military spenders publicly stating that they possess (or are in the process of developing) offensive cyber capabilities[106] (as an aside, the majority of cyber-attacks, reportedly, originate in States around Eastern Europe and Eastern Asia).[107]

With this increased prevalence of offensive cyber strategies appearing in State publications, States have expended significant resources to ensure that their cyber defences are

[99] Global Sign "Six Cybersecurity tools and services every business needs" (Globalsign, 28 August 2018) online: <https://www.globalsign.com/en/blog/six-cybersecurity-tools-and-services-every-business-needs/>
[100] Government of Canada, *supra* note 54 at 5.
[101] *Ibid*.
[102] APCO Worldwide, "China's 12th Five-Year Plan: How it actually works and what's in store for the next five years" at 3 (Washington, DC: December 10, 2010) online (pdf): <http://www.apcoworldwide.com/content/pdfs/chinas_12th_five-year_plan.pdf>
[103] US Government, *supra* note 42 at 215.
[104] E Burger, G Bordacchini, *supra* note 2 at 10
[105] D Sanger, N Perlroth, U.S. Escalates Online Attacks on Russia's Power Grid (NY Times, Jun 15, 2019), <https://nyti.ms/2KiTwMl>
[106] J Lewis, G Neuneck, *supra* note 23 at 2.
[107] UNODC Study on Cybercrime, *supra* note 24 at 49.

suitably fortified.[108] With State actors being both well trained in exploiting the intricacies of computer networks[109] and well provided with resources for continuous, coordinated attacks,[110] defensive measures must be agile enough to dynamically reshape operations and maintain mission continuity even while under continuous attack.[111]

e) The issue of insiders

One of the most worrisome concerns is that of an "insider" – a person who has authorised and legitimate access to a system or network, who utilizes that access, intentionally or unintentionally, to facilitate an attack to that network.[112] This threat is separate from those potential perpetrators mentioned above (individual hackers, criminal organisations, terrorists, and States), in that insiders are not only a threat in and of themselves (potentially belonging to any of the aforementioned groups), but in that they can also be utilised by those above-mentioned perpetrators to achieve a goal, through means such as exploitation of poor practices, threats, or bribery.

In mentioning 'insider attacks', most likely the first thing which springs to mind is the malicious and intentional insider who deliberately tampers with satellite controls or introduces malware to a system. However, in addition to deliberate insiders, there is also the very real risk of a non-malicious employee who unintentionally introduces malware to a system.[113] This is particularly pertinent because roughly 36% of the worst security breaches are reportedly caused by inadvertent human error, while only 10% are due to a deliberate misuse of systems by staff.[114] This risk is increased during the installation of new equipment, or during the upgrade

[108] As an example, the UK expressed that , a small number of foreign actors have developed offensive, and potentially destructive, cyber capabilities which could threaten the security of the UK's critical national infrastructure and industrial control systems , as per HM Government, *supra* note *77* at 18.
[109] Poloalto Networks "What is Cybersecurity?" <www.paloaltonetworks.com>
[110] CANSO, *supra* note 84 at 5.
[111] CANSO, *supra* note 84 at 5
[112] *Ibid* at 4.
[113] Y Lipkin, *supra* note 37 at 36
[114] C Hurran, Cyber Insiders: A Board Issue (Cyber security Review, Publication Date May 2015) online: <http://www.cybersecurity-review.com/articles/cyber insiders-a-board-issue/>

of software or firmware of an existing device, as these often require the admittance of a technician, who introduces non-authorised external devices and employs non-standard protocols and operating-systems, thereby allowing a potential attacker easy access to the station, either with the intentional or unintentional assistance of the technician.[115]

The concern that insiders pose to cyber security has been highlighted in a number of States' cyber security plans (with a heavy emphasis on the intentional and malicious insiders, as clearly the issue of unintentional insiders is a separate issue, which is better combatted by simply ensuring a robust cyber security culture). There is a pronounced importance to establish a dedicated personnel security culture which is alert to the threat posed by disaffected employees, fraud in the workforce, and industrial and other forms of espionage.[116]

f) Summary

As a result of the ever-growing cyber literacy in all sectors of society, cyber-attacks are becoming easier to carry out, are occurring more often, and are being perpetrated by a wider range of actors. These attacks have a demonstrated ability to cripple critical pieces of national infrastructure and, given societies dependence on cyber technologies in nigh every aspect of day-to-day life, it should come as no surprise that cyber security is now a key priority for industry and government alike. In line with this, the next Part of this thesis will look at cyber security best practices within States, with a view to determining how such best practices can be incorporated into a new international instrument.

[115] HM Government, *supra* note *77* at 19.
[116] HM Government, *supra* note *77* at 19.

PART II

'WITHIN-STATE' BEST PRACTICES

While the focus of this thesis is directed towards how international dialogue can help to curb the risk that cyber-attacks pose to outer space assets, it is important to examine existing practices within States, as this helps to determine the viability of options at an international level, and also determines the amount of capacity building and assistance that may be available from (or required by) States. In this Part, therefore, we will be looking first at industry level cyber security practices, and then moving to how domestic policy and practices help to curb cyber risks.

A. Industry level cyber security

As of 2019, Cyber security Ventures estimated that the global cyber security market is worth an estimated $USD 120 billion.[117] While this figure may sound intimidatingly large, the fact that cyber-crime is expected to cost companies up to $USD 6 trillion by 2021[118] demonstrates that, if anything, industry is undervaluing the importance of having a robust cyber security regime. With that being said, the private sector is now reporting a new level of cyber security awareness, conducting some degree of cyber-crime risk assessment, and utilizing forms of cyber security technology in essentially all large corporations.[119]

We will now discuss some of the initiatives undertaken by private sector to protect their assets. Note, however, that such cyber security measures do not need to be designed and implemented by the organization themselves, but are instead often established by contracted cyber security professionals. Regarding space-based assets specifically, the United States-based company 'RT Logic' provides cyber protection for ground stations, satellite test equipment, and satellite operations, boasting a high success rate in a large number of different

[117] S Morgan, *supra* note 2.
[118] *Ibid*.
[119] UNODC Study on Cybercrime, *supra* note 24 at 239.

space missions.[120] On similar lines, Israel Aerospace Industries provides defence forces, governments, critical infrastructures, and large enterprises with end-to-end cyber security and monitoring tools.[121]

1. General cyber security

Cyber-attacks are not necessarily always sophisticated, but are often just the result of easily rectifiable, and most often preventable, vulnerabilities.[122] Most cases analysed in cyber security studies do not involve complex skills or techniques, but can be prevented with simple cyber security.[123] Such simple cyber security measures include such tools as:[124]

i. Firewalls - these monitor network traffic as well as connection attacks, and determine access to a computer or network;

ii. Antivirus software – in addition to alerting users to virus and malware infections, such software can also quarantine and remove these threats, and perform services such as scanning emails to ensure they are free from malicious attachments or web links;

iii. Secure Sockets Layer (SSL) – SSL is responsible for encrypting server communications, providing the HTTPS and padlock which customers see in their browser address bars.

iv. Public Key Infrastructure (PKI) – Amongst other things, PKI carries out multi-factor authentication and access control, creating digital signatures to authenticate signer's identity, as well as encrypting email communications.

For a business to reduce its exposure to potential cyber harm, it needs to balance the risk to critical systems and sensitive data from cyber-attacks against how much it can afford to

[120] RT Logic "About Us" (2017) <www.rtlogic.com>
[121] Israel Aerospace Industries "Cyber Solutions: End-to-End Cyber Solutions" <http://www.iai.co.il>
[122] HM Government, *supra* note *77* at 22.
[123] UNODC Study on Cybercrime, *supra* note 24 at 42-43.
[124] Global Sign, *supra* note 99.

invest in people, training, technology and governance.[125] Factored into this balancing, industry needs to realize that cyber security is a constant investment, wherein cyber defences are regularly tested and upgraded accordingly.[126]

2. Cyber Hardening

In high risk and high security industries such as outer space, reducing the various vectors of vulnerability is crucial. Cyber hardening is a process whereby a system is secured by reducing its surface of vulnerability by removing all non-essential software programs and utilities from a computer. At an advanced level, this may involve reformatting the hard disk, and only installing the bare necessities that the computer needs to function.[127]

3. Insider Attacks

As mentioned above at [*Part I(A)(2)(e)*], insiders are a key concern for industry and governments alike. In order to effectively mitigate this risk (commonly referred to as Cyber Insider Risk Mitigation or 'CIRM') an organization needs to manage this issue in a holistic and not exclusively technical manner, all whilst ensuring that such CIRM measures to not negatively impact business delivery.[128]

As a key starting point, by ensuring CIRM responsibilities are held by a single, board-level owner who fully integrates CIRM processes into the corporation's security stratagem, a corporation can ensure a comprehensive oversight over the risk which insiders pose.[129] This single owner must make certain that CIRM measures are adaptive, implemented across the whole business (and integrated into the business culture), and that they take into account the

[125] HM Government, *supra* note *77* at 22.
[126] C Johnson, *supra* note *22*.
[127] International Organization for Standardization ISO/IEC 27001, at 2 (Interdisziplinarer Normenbereich Sectur interdisciplinaire de normalisation, 2013) online (pdf): <https://trofisecurity.com/assets/img/iso27001-2013.pdf>
[128] C Hurran, *supra* note 114 at 3.
[129] C Hurran Cyber Insider Risk Mitigation Maturity Matrix, at 2-6 (Cyber Security Review, Autumn 2016) online (pdf): <http://www.cybersecurity-review.com/wp-content/uploads/2016/11/Chris-Hurran-article-CSR-Autumn-2016.pdf>.

tangible, intangible, and information assets which are at risk during a cyber-attack.[130] Equally as important, the business must ensure both transparency and awareness, through measures such as implementing corporate pre-employment and periodic screening policy and procedures, as well as comprehensive exit procedures for ex-employees.[131] All of these measures should, ideally, be implemented both up and downstream through a supply chain, though this will be discussed further at [*Part II(A)(5)*].

In addition to prevention, CIRM also requires a response plan for when such attacks do occur, ensuring that processes are in place to minimise harm, protect the operation, assets and reputation, and to detect, identify and prosecute insiders.[132]

4. Training and compliance

As mentioned at [*Part I(A)(2)(e)*], the issue of unintentional insiders (those who, through lack of training or oversight, unintentionally allow malicious outsiders access to their industries database) is a fundamental concern. To rectify this, formal training is required, developing specialist skills and capabilities which allow employees to keep pace with rapidly evolving technology and associated cyber risks.[133]

Training and compliance is particularly important as, reportedly, more than 90 percent of successful hacks and data breaches stem from email phishing scams, and training employees how to detect and react to such threats is a low-cost and high-reward investment.[134] Additionally, banning all personal devices from control rooms, and disallowing the attachment of external devices to all but a few well-monitored access points are all basic but important steps which can be taken to severely reduce the risk of a cyber intrusion to a system.[135]

[130] C Hurran, *supra* note 129 at 3.
[131] *Ibid* at 4.
[132] C Hurran, *supra* note 114 at 4.
[133] HM Government, *supra* note 77 at 22.
[134] S Morgan, *supra* note 2.
[135] C Baylon, *supra* note 22 at 12.

5. Supply chain management

Ensuring that every aspect of a supply chain maintains similarly strict cyber security policies is particularly important. As this relates to outer space assets, this would mean ensuring that internet services and hosting providers, and those who provide both hardware and software (in the ground stations, and outer space assets themselves) have sufficiently stringent security protocols, and that they can be held accountable if this is not the case.[136] Such supply chain management can often be done through including minimum cyber standards and accountability paragraphs within procurement contracts – a practice which is widely utilised in both industry and government procurement globally.[137]

6. Pursuing civil remedies

While not strictly 'security', some industry participants have taken proactive steps to discourage and remedy the consequences of cybercrime, utilizing (and threatening the use of) civil law mechanisms.[138] The broadening of legal action beyond criminal action is important, particularly in instances where criminal liability cannot be attributed to a specific perpetrator (i.e. when attributed to a State or a company) or when the financial implications of that attack are significant.

7. Summary

Throughout history, industry collaboration has been a key aspect in developing government technology, and one would envisage that the issue of cyber security will be no different. Industry is also playing a bigger part in multi-stakeholder, bottom up activism, as exemplified in the active stance by the Microsoft Corporation in the Digital Geneva Convention,[139] wherein Microsoft voluntarily committed to 'act responsibly, to protect and

[136] UNODC Study on Cybercrime, *supra* note 24 at 239.
[137] *Ibid.*
[138] *Ibid.*
[139] Microsoft, "A Digital Geneva Convention" online (pdf): <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW67QH>

empower… users and customers, and thereby to improve the security, stability, and resilience of cyberspace'.[140]

As an aside (and not particularly industry specific), academic institutions play an important role in cyber-crime prevention through developing and sharing knowledge, assisting in legislation and policy development, developing technology and technical standards, delivering technical assistance, and cooperating with law enforcement.[141]

B. Domestic policy

The ITU's Global Cybersecurity Index report of 2018 demonstrates that cybercrime legislation is present in approximately 91% of all States (up from 79% in 2017)[142] and that the majority of States (58%) reported have a national cybersecurity strategy (NCS).[143] While it is clear that cyber-policy is present in a large number (and wide range) of States, there is not uniform best practice as to how such policy should be drafted or implemented, and as such there remains significant discrepancies between State security approach in this field.

This section will look toward a variety of these State policies, building a global cross-section of best practices to protect key pieces of national infrastructure. To do so, the discussion draws on the 2012 ITU/CARICOM/CTU policy guidelines and legislative texts, which were proposed to help develop and harmonize policies between States.[144]

1. Establishing of a cyber focused government body

While every Government agency tends to have it's own dedicated cyber department (to varying sizes and independence, generally depending on funding), given industry and

[140] Tech accord, "CYBERSECURITY TECH ACCORD" (accessed 02 December 2019) online: <https://cybertechaccord.org/accord/>
[141] UNODC Study on Cybercrime, *supra* note 24 at 239.
[142] Europe and the CIS regions stand out as having the highest number of countries with national strategies, and the Africa region shows the lowest number (14 out of 44 countries having a NCS). See ITU, Global Cybersecurity Index (GCI) 2018 at 18 (ITU Publications, 2018) online (pdf): <https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf>
[143] *Ibid* at 17.
[144] ITU, Harmonization of ICT Policies, Legislation and Regulatory Procedures in the Caribbean (2012) online (pdf): <https://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/reports/wg2/docs/HIPCAR_1-5-B_Model-Policy-Guidelines-and-Legislative-Text_Cyber-crime.pdf> [ITU/CARICOM/CTU Model Legislative Texts]

government's reliance on cyber connectivity (and the corresponding threat that cyber-attacks pose), there is now a convincing argument to be made that a dedicated cyber security agency needs to be formed as a part of any government that wishes to protect its assets. This cyber focused government agency should also encourage and coordinate cross-sectoral collaboration between other agencies within government, as this is crucial to ensure a cross-cutting and efficient domestic cyber security regime.[145]

In line with this, we have seen State's start to agglomerate their separate agency cyber security departments into one central body, sharing their experience and pooling their resources. Finland, for example, has roles divided in several sectors, with aspects of cyber security divided among communication, transport, and the "Suojelupoliisi" (the country's security intelligence service). Finland's most recent National Cyber Security Strategy, however, supports the creation of a centralised command organisation with direct oversight and full decision-making responsibility to manage cyber domain threats.[146]

Separately, in 2011, Australia developed the Protocol for Law Enforcement on Cyber-crime Investigations which sought to identify the most appropriate agency to deal with a cyber-crime matter, taking into account the different kinds of cyber-crimes, the nature and location of victims and offenders and a number of other contextual factors.[147] Following from this, in 2013, the Australian Government announced that it would establish the Australian Cyber Security Centre (ACSC), bringing together the Government's cyber security capabilities in a single facility.[148]

---

[145] E Burger, G Bordacchini, *supra* note 2 at 41

[146] G O'Dwyer Finland Government examines centralised cyber defence (Computer Weekly, 22 May 2018) online: <https://www.computerweekly.com/news/252441613/Finland-government-examines-centralised-cyber defence>

[147] Australia, Australian Attorney-General's Department "National Plan to Combat Cyber-crime at 17 (accessed 06 June 2019) online: <https://sherloc.unodc.org/res/cld/treaties/strategies/australia/_html/national-plan-to-combat-cyber-crime_2013.pdf>

[148] *Ibid* at 15.

The trend towards centralization of State cyber defence and research provides a more complete understanding of threats across the cyber spectrum, facilitating faster and more effective responses to serious cyber incidents, and enabling a more cohesive interaction between governments, industry, and international partners.[149]

2. Legislating against acts which constitute cyber-crime

The principle of *nullum crimen sine lege* requires that the conduct constituting any criminal offence must be described clearly by law. Clearly then, the first step in establishing a comprehensive domestic cyber security regime is identifying those acts which constitute cyber-crimes.[150] In addition to reducing the prevalence of cyber-crime in one's own home State, this inspires confidence in other States, confirming to them that the actor takes the threat of cyber-attacks seriously, and assures them that that actor is engaged in the common battle against cyber-crime. Most States have some consistent baseline of acts which they consider to be culpable cyber-crime conduct. These can generally be separated into several key areas, including:[151]

i. Acts against the confidentiality, integrity and availability of computer systems – Such acts would include illegal access to computer systems, illegal interception or acquisition of data, and interference with computer systems. Criminalization of these acts has existed since the earliest days of the development of information technologies, representing an important deterrent. Roughly 70% of States incorporate illegal access into their cyber legislation with most requiring that the

[149] Australia, *supra* note 147 at 15.
[150] UNODC Study on Cybercrime, *supra* note 24 at 11-12.
[151] Note: only those policies which can have a direct bearing on the safety of outer space assets will be mentioned (and thus we will not be discussing legislation which relates to issues such as computer-related acts for personal or financial gain or harm, including fraud, forgery, acts against children etc.). See UNODC Study on Cybercrime, *supra* note 24 at 16.

interference be intentional (with only a limited few States criminalizing reckless interference);[152]

ii. Illegally remaining in a computer system – If a State is to criminalize illegal access to a computer system, it is important that that State also criminalizes illegally 'remaining' in a computer system.[153] This relates to circumstances where, for example, a technician is permitted access to a system for the purposes of updating or installing new software or hardware – once that task is complete, it is important that the technician is mandated to exit that system and to relinquish any control over the system;

iii. Ownership of tools which can be used for computer misuse – This issue is a tremendously difficult one to legislate, considering the fluid boundary between 'preparation' for and 'attempt' at a criminal offence, as well as the problem of 'dual-use' objects, which may be used for either innocent or criminal purposes. While not all States criminalize computer misuse tools, among those that do, differences arise regarding whether the offence covers possession, dissemination, or use of software (such as malware) and/or computer access codes (such as victim passwords).[154]

To avoid over-criminalization, many States ensure that provisions on computer-misuse tools not only require that that tool is designed for the commission of an offence, but also that the perpetrator intended to use it for that purpose.[155] Such 'intentionality' provisions are important to ensure that negligent or reckless acts do not warrant disproportionate criminal sanctions.[156]

[152] UNODC Study on Cybercrime, *supra* note 24 at 79-82.
[153] ITU, *supra* note 144.
[154] UNODC Study on Cybercrime, *supra* note 24 at xx.
[155] *Ibid* at 106.
[156] ITU, *supra* note 144 at 11.

Participating in research and development of cyberweapons is also an area which has been considered for criminalization, however this is generally set aside as impractical given that it is nearly impossible to verify;[157]

iv. Mandating private sector assistance – In order to help facilitate investigation of cyber-crimes, some States have started to mandate for technology providers to 'assist' law enforcement. These have taken the form of legislatively mandated 'encryption backdoors'[158] which allow law enforcement access to a system to investigate serious breaches of the law.[159] In line with this concept, some countries (i.e., France, Germany)[160] have supported legislation to compel technology and communications companies to decrypt customers' data,[161] while others (the Netherlands, Estonia)[162] have voiced support for strong encryption.

Recent domestic regulation[163] has also mandated minimum standards for industry in terms of design security and resilience. This is a notable shift from the traditional approach of end-user responsibility.[164]

---

[157] J Lewis, G Neuneck, *supra* note 23 at 136.
[158] There are calls for EU level regulation on this issue. See: Iain Thomson, "Germany, France lobby hard for terror-busting encryption backdoors – Europe seems to agree" (The Register, February 2017) online <https://www.theregister.co.uk/2017/02/28/german_french_ministers_breaking_encryption/>.
[159] Citizen Lab, 'Shining a Light on the Encryption Debate: a Canadian Field Guide' (The Citizen Lab and the Canadian Internet Policy & Public Interest Clinic, May 2018) online (pdf): <https://citizenlab.ca/wp-content/uploads/2018/05/Shining-A-Light-Encryption-CitLab-CIPPIC.pdf>
[160] German and French joint letter by Ministers of the Interior (February 2017) See: B Acharya, K Bankston, R Schulman, A Wilson "Deciphering the European Encryption Debate: France" at 10 (Open Technology Institute, August 2017) online (pdf): <https://na-production.s3.amazonaws.com/documents/France_Paper_8_8.pdf>
[161] Brian Barret "The Apple-FBI Battle is Over, but the New Crypto Wars have Just Begun" (Wired, March 2016) online: <https://www.wired.com/2016/03/apple-fbi-battle-crypto-wars-just-begun/>
[162] Netherlands, Cabinet position on encryption (April 21, 2016) online: <https://www.enisa.europa.eu/about-enisa/structure-organization/national-liaison-office/news-from-the-member-states/the-netherlands-cabinet-launched-position-on-encryption>; Estonia, Estonian Information System Authority position (Estonian Annual Cyber Security Assessment, 2018) at 38-40. Both view strong encryption as fundamental to the functioning of the digital society and national digital ecosystem, not merely a security vs privacy dilemma.
[163] As an example, see: EU, Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (27 April 2016) online: <https://publications.europa.eu/en/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1/language-en>
[164] CCDCOE, Trends in international law for cyberspace, at 4 (NATO, May 2019) online (pdf): <https://ccdcoe.org/uploads/2019/05/Trends-Intlaw_a4_final.pdf>

While the above-mentioned acts are, to some degree, widely criminalised, States show wide divergencies in national approaches to the penalties associated with cyber-crime acts (for example, examination of the crime of 'illegal access' shows considerable difference in its perceived seriousness between States, ranging from a misdemeanour to a potentially extraditable act),[165] causing clear issues in cases of transnational cyber-crime. Particularly when considering such prevalently cross-border issues as outer space and cyber space, ensuring consistency of criminal acts (and associated sanctions) between States should be a priority.

Another significant issue in domestic policy on cyber-crime is the almost universal focus on criminalization in domestic legislation, with some remarking that this ignores many other key factors which can help manage these risks and deter attacks, such as procedural powers, jurisdiction, international cooperation, and internet service provider responsibility and liability[166] (this focus on criminalization, for example, includes the US,[167] New Zealand,[168] and Canada).[169] Such a focus, it has been suggested, arises from the fact that cyber legislation still maintains roots in the 19th century legislation from which it was adopted, focusing around physical objects without taking into account the particularities of cyber-crime and crimes generating electronic evidence.[170]

Though departing from traditional forms of policy is often both difficult and resource intensive, if cyber space is going to be effectively regulated, States will need to invest in devising a revised and flexible legal regime which responds to the unique and wide-ranging threats which cyber-attacks pose at the rapid rate that is required.

---

[165] UNODC Study on Cybercrime, *supra* note 24 at 56.
[166] C Baylon, *supra* note *22* at 12.
[167] US, Code of Federal Regulations, 14 U.S.C. §§1030, 1037 2701
[168] New Zealand, Crimes Act, s249-252 (1961)
[169] Canada, Criminal Code, art. 430 (1985)
[170] UNODC Study on Cybercrime, *supra* note 24 at 51.

3. Implementation of cyber policy: Investigation and gathering of evidence

It is not enough to criminalize cyber activities if State authorities are unable to effectively investigate those crimes, and gather evidence for judicial processing. Ensuring that procedural measures are in place to effectively move such cases through the criminal justice system is critical in this regard.

a) Investigation of cyber-crime

By implementing effective investigative procedures for cyber cases into standard operating protocol for law enforcement, States can effectively deter potential perpetrators, and help to facilitate international cooperation in regards to transnational cyber-crime (which, as mentioned, is an inherent part of both outer space and cyber space).

Investigative challenges in this area arise from difficulties in accessing electronic evidence (particularly as a large part of the infrastructure and computer systems used for internet communications is owned and operated by the private sector), and from internal resource, capacity and logistical limitations, as well as the fact that suspects frequently use anonymization and obfuscation technologies.[171]

To help develop investigative capabilities of cyber-crime, the Australian Government has placed a significant focus on building capacity of law enforcement agencies to investigate cyber-crime, encouraging basic training on cyber-crime and digital evidence in policy training (expertise from the private and tertiary sectors is also used to develop these capabilities, such as through secondments).[172] Further, the Australian Government has released a national plan to combat cyber-crime which focuses on building the capacity of the Australian Cyber-crime Online Reporting Network to refer reports to law enforcement agencies, and explores other mechanisms to improve cooperation on cyber-crime matters across Australian jurisdictions

[171] UNODC Study on Cybercrime, *supra* note 24 at xxi.
[172] Australia, *supra* note 147 at 31.

through the National Cyber-crime Working Group and the Australia/New Zealand Policing Advisory Agency (ANZPAA) e-Crime Working Group.[173]

Additionally some States have, in cases of serious crime, suggested that there should be provisions enabling competent authorities to make use of sophisticated investigation instruments such as key-loggers and remote forensic software to collect passwords used by suspects.[174] In pursuit of this line of thinking, a number of States have also begun to allow real-time collection of computer data, either through a general or cyber specific power, or through an extension of general 'telecommunications intercept acts' or 'eavesdropping laws.'[175]

b) Digital Forensics

As part of investigating and gathering evidence of cyber-crime, 'Digital Forensics' is the process of using computer science and investigative procedures to recover evidentially important information. This information can potentially be quite complex, requiring sophisticated techniques to recover traces of activity or data from computers and networks,[176] and can exist in the form of computer files, transmissions, logs, metadata, or network data.[177]

As an example of digital forensics being incorporated into domestic policy, similar to the 'central cyber focused government body' mentioned in [*Part II(B)(1)*], some States have established central 'forensic laboratories' which expertly analyze electronic evidence been seized by policy investigations, while other States have established forensic units throughout the State, utilizing specialised forensic tools on networks, computer systems, storage devices and cellphones as required.[178]

---

[173] *Ibid*.
[174] ITU, *supra* note *144*.
[175] UNODC Study on Cybercrime, *supra* note 24 at 131.
[176] L Daniel, Digital Forensics for Legal Professionals: Understanding Digital Evidence from the Warrant to the Courtroom (1st Ed., Syngress, 2011) at 3
[177] UNODC Study on Cybercrime, *supra* note 24 at xxiii.
[178] *Ibid* at 178.

Given the importance of these techniques, coupled with the fact that many States, across all regions, have reported having an insufficient number of forensic examiners, lack of forensic tools, and backlogs due to overwhelming quantities of data for analysis,[179] this could be identified as an area for capacity building.

c) Gathering and storing evidence

In addition to investigating cyber-crime, law enforcement must be able to effectively transmit evidence to the judiciary for prosecution. While traditional criminal investigative procedures contains provisions for the gathering and admitting evidence, electronic evidence is easily altered, thus making it important to ensure the integrity, authenticity, and continuity of evidence throughout the entire time period between its seizure and its use in trial (i.e. the chain of custody).[180] In this regard, it is also important that evidence continuity be maintained for both the physical device housing the data (when received or seized), and the stored data residing on the device.[181] Mauritius has provided an interesting solution to this issue by utilizing a 'preservation order' which states that "any investigatory authority may apply to the Judge in Chambers for an order for the expeditious preservation of data that has been stored or processed by means of a computer system or any other information and communication technologies, where there are reasonable grounds to believe that such data is vulnerable to loss or modification."[182]

While it is important to always consider the need to maintain integrity of potential evidence, it is also important to note in these cases that the adaptation of traditional and coercive measures (such as search and seizure) to cyber investigations is largely unfeasible, due both to the volume of individual cases investigated, as well as due to the disruption to

[179] UNODC Study on Cybercrime, *supra* note 24 at xxiii.
[180] *Ibid*.
[181] *Ibid* at 158.
[182] Mauritius, Computer Misuse and Cyber-crime Act, Part III, s11 (2003) online (pdf): <http://www.ncb.mu/English/Documents/Legislations/Computer%20Misuse%20and%20Cyber-crime%20Act%202003/misuse.pdf>

legitimate business activity.[183] If such search and seizure instruments are to apply to this new environment of cyber space, they will need to be recrafted to relate to digital evidence and computer technology in a way which avoids the collection of evidence being questioned for authenticity.[184]

What is required in law enforcement as it relates to cyber-crime, then, is that it requires a combination of both traditional and new policing techniques. While traditional investigative actions can be effective, many now require a transition from a spatial, object-oriented approach, to one involving electronic data storage and real-time data flows.[185]

4. Judicial processing of cyber-crime

Ensuring that capacity is built throughout the whole judicial process is another key aspect to implementing cyber policy. This includes ensuring that both counsel and judges are literate in cyber matters, and also that there are processes for evidence to be admitted into the judiciary.

a) Ensuring cyber literacy in judiciary

The vast majority of cyber-crime cases are handled by non-specialised judges, with about 40% of countries responding to a UNODC study stating that their judges do not receive any form of cyber-crime related training.[186]

So too is there a lack of cyber-literacy amongst counsel, with all countries in Africa, and approximately one-third of countries in other regions reporting that they have insufficient resources to train their counsel to view and understand electronic evidence to build a case at trial.[187]

[183] UNODC Study on Cybercrime, *supra* note 24 at 128.
[184] ITU, *supra* note 143 at 12.
[185] UNODC Study on Cybercrime, *supra* note 24 at xxii.
[186] *Ibid* at xxiii.
[187] *Ibid.*

Accordingly, Australia emphasizes the Government's role in providing resources to respond to legal concepts associated with new technology and the facilities needed to analyse and consider digital evidence in a court setting,[188] with the Australian Federal Police proactively providing training workshops for the legal community and developing mechanisms to improve the presentation of digital evidence in courts, particularly through the development of the e-Court facility.[189] In addition to this, Australia has focused on establishing an effective framework for investigation and prosecution of cyber-crime, putting emphasis on providing adequate training for prosecutors and judicial officers to help them to consider digital evidence and to understand and present highly technical details in order to effectively administer the law.[190]

b) Procedural instruments for judicial processing of cyber-crime

In addition to ensuring that judges and lawyers are trained in terms of how to review cyber evidence, it is important to ensure that that evidence is available for them to review in the first instance. Cyber evidence has been presented in Court through testimony delivered by police officers or forensic practitioners, including presentation of digital information on projectors and widescreen monitors, and through printouts identifying objects, documents, photographs, logs, and screen captures.[191]

While these are good practices, they are not commonplace, with less than 40% of States regulatory frameworks making legal distinction between electronic and physical evidence.[192] This lack of a distinction can make it difficult to legally attribute a cyber-crime act to a perpetrator, as the principles of best evidence, relevance of evidence, hearsay, authenticity of

[188] Australia, *supra* note 147 at 23.
[189] *Ibid* at 22.
[190] *Ibid.*
[191] Commonwealth Model Laws on Computer and Computer-related Crime and Electronic Evidence (2002), Part III(11); UNODC Study on Cybercrime, *supra* note 24 at 167.
[192] Note: 85% of countries have stated that electronic evidence is admissible in criminal proceedings. Those locations where it is inadmissible are predominately in Africa and Asia: As per UNODC Study on Cybercrime, *supra* note 24 at 165.

evidence, and integrity of evidence are not easily transferrable to the 'non-physical' realm of cyber space.[193]

5. Interacting with the private sector

The private sector is often the first to become aware of emerging cyber-crime threat, making them an important port-of-call for any government looking to stay ahead of the rapidly changing cyber threat vectors. Clearly, there are policy reasons which limit the extent to which public and private sectors can collaborate (ie. privacy or security concerns), but striking that balance is crucial if a State is to effectively regulate and mitigate the risks of cyber-attacks against its assets.[194]

Such public-private partnerships, created both by informal agreement and by legal basis, are used for facilitating the exchange of information on threats and trends, and also for prevention activities, and action in specific cases.[195] Additionally, private sector entities have taken proactive approaches to investigating and taking legal action against cyber-crime operations, complementing actions of law enforcement and mitigating damage to victims.[196]

Australia places significant emphasis on partnering with industry, encouraging industry-led arrangements to protect against the impact of cyber-crime, exploring options to increase information-sharing with industry on cyber threats and vulnerabilities, and increasing cooperation on mutually-beneficial research and development initiatives designed to better understand and minimize cyber-crime.[197] Furthermore, the Australian government has taken several steps toward this private-public partnership with its Computer Emergency Response Team (CERT Australia) working with the private sector to provide cyber security assistance and to share information on cyber threats and incidents.[198]

---

[193] UNODC Study on Cybercrime, *supra* note 24 at xxiv.
[194] Australia, *supra* note 147 at 15.
[195] UNODC Study on Cybercrime, *supra* note 24 at xxvii.
[196] *Ibid* at xxvii.
[197] Australia, *supra* note 147 at 29.
[198] *Ibid* at 15.

The United Kingdom also emphasizes the importance of supporting start-ups and innovation as it relates to the cyber sector, utilizing levers such as the General Data Protection Regulation (GDPR),[199] to drive up standards of cyber security across the economy, including through regulation.[200] The UK focus extensively on building strong relationships with non-government actors, whether that be industry, civil society, academia, or the technical community, stating that these relationships are crucial to inform and challenge international policy formulation, and to strengthen political messages on a wide range of cyber issues.[201]

While the very partnership-centric approach of Australia and the UK is extremely valuable, it is also important that minimum standards are set for private standard where lack of such standards could have negative impacts outside of that private entity. In this regard, the European Union have stressed the importance of setting mandatory standards for private sector participants. Following a proposal by the European Commission, the European Union introduced legislation, changing their privacy laws to strengthen and unify data protection for individuals in the EU.[202] These changes also addressed the export of personal data outside the European Union, and stated that the penalties and fines for the most egregious violations could be up to 4% of an enterprise's revenue.[203] The importance of this new privacy legislation should not be understated. By broadening the scope of the Regulation to apply this to data controllers established outside the Union when data processing, the legislation has a significant

[199] The General Data Protection Regulation (EU) 2016/679 is a regulation in EU law on data protection and privacy for all individual citizens of the EU, which also focusses on the transfer of personal data outside of the EU.
[200] HM Government, *supra* note 77 at 27.
[201] *Ibid* at 64.
[202] Office Journal of the European Union, Regulation (EU) 2016/679 of the European Parliament and of the Council (27 April 2016) at [2] & [103], online: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN>
[203] *Ibid* at 83(4).

effect on non-European internet service providers, ensuring the protection of assets across borders.[204]

a) Educating civil society to protect themselves

While it might not be the most intuitive step, helping civil society to guard against cyber-crime risks can have an "upflow" effect to sectors of government and the protection of critical infrastructure. By taking such actions like encouraging all sectors to include cyber protection into their induction programs, establishing a government hotline for cyber security issues, or releasing public service programs advising how to make one's personal computer more secure, a Government is able to reduce the overall amount effective malicious cyber instruments in cyber space, and ensure that the public (who may eventually be Government employees) are educated in regards to good cyber security practices (thereby reducing the risk of employing an 'unwitting insider' as discussed at [*Part I(2)(e)*]).

Australia places a significant emphasis on ensuring civil society is 'cyber smart', implementing a national online reporting facility for cyber-crime (the Australian Cyber-crime Online Reporting Network or 'ACORN'), which provides Australians with a national point-of-contact to receive reports of cyber-crime, provides access to general educational advice, and refers reports to law enforcement and government agencies for further consideration and possible investigation.[205] New Zealand also focuses extensively on increasing awareness to the general public to promote online security, stating a clear objective in its cybersecurity strategy of raising understanding and awareness among small businesses and individuals.[206]

Finland, too, emphasizes the importance of a consistent dialogue between the public and civil sectors, citing dialogue of this kind as one of the reasons for Finland being a global

[204] M Papa, "Regulation (EU) 2016/679: how the European personal data protection landscape will change" (European Union, May 31, 2016) online: <https://www.lexology.com/library/detail.aspx?g=27ae467a-e2ed-4efc-ba4d-16d74c95e661>
[205] Australia, *supra* note *147* at 28.
[206] New Zealand Government, New Zealand's Cyber Security Strategy, 2011, p. 6.

frontrunner in cyber threat preparedness.[207] Finland has further proclaimed that it views cybersecurity as an issue which needs be tackled by society as a whole, going so far as to establish a Cyber Security Centre and 24/7 information security arrangement for the entire society.[208]

6. Encouraging the sharing of information

Tied to the concept of maintaining a flexible and adaptable cyber security regime is a very important principle – information, whether it be about threats or best practices, must be shared within the industry, across the supply chain, and with governments.[209] By ensuring that information and threats are shared effectively, both States and industry obtain an accurate assessment of the threat which cyber-attacks pose, and an idea of what the latest threats are or might be. The reason that enforcing such information sharing requirements tends to be so difficult is that organizations are often concerned about the risk of reputational harm, and about the risk of information being misused, putting them further at risk.[210] For an indication as to the extent of this apprehension, the FBI's Internet Crime Complaint Center stated that the number of reported cyber-crimes in the agency's reports represents approximately 15 percent of the total number of such offences actually committed in the U.S. each year.[211]

Numerous States have attempted to rectify this underreporting of cyber-crime through legislation. Australia, notably, announced in its 'National Plan to Combat Cyber-crime' that fostering an intelligence-led approach, as well as information-sharing, were priorities in the national response to cyber-crime.[212] The United States has also taken a significant step towards this goal, and is in fact the only State to have released any information on its so-called

[207] Secretariat of the Security Committee, Government Resolution: Finland's Cyber security Strategy (24 Jan, 2013) at 3, online (pdf): <https://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf>
[208] *Ibid* at 5.
[209] PriceWaterhouseCoopers, Aviation perspectives: 2016 special report series: Cybersecurity and the airline industry – part 2 of 4: Prevention (PWC, 2016) at [1], online (pdf): <https://www.pwc.com/us/en/industrial-products/publications/assets/pwc-airline-industry-perspectives-cybersecurity-prevention.pdf>
[210] S Morgan, *supra* note 2.
[211] IC3, *supra* note 34 at 5
[212] Australia, *supra* note *147* at 30.

'Vulnerabilities Equities Process' (VEP)[213] which is a process whereby the US federal government determines, on a case-by-case basis, how it should treat newly discovered and not publicly known vulnerabilities in information systems and technologies (ie. whether to disclose them to the public to improve general computer security, or to keep them secret for official offensive and defensive purposes).[214]

7. Constant innovation

By its very nature, cyber-attacks are a fast-moving and adaptive threat, forever on the leading edge of technology. For every gap which is blocked, there are actors looking to discover and exploit a new one. In order to combat the fast-moving nature of cyber threats, States and space programs alike must constantly monitor and evolve their cybersecurity programs to keep pace with the varying and adaptive threat vectors. Constant innovation and monitoring is crucial if an organization is to ensure early detection of intrusions, thus reducing the consequences of the attack.[215]

The United Kingdom's 2011 National Cyber Security Strategy, as an example, placed significant focus on responding to the evolving cyber threat, focusing on research and development and on cutting-edge analysis to overcome future threats and challenges.[216]

8. Legislation surrounding outer space assets, critical infrastructure and terrorism

The most fundamental step to protecting an outer space asset from attack will be to make it an offence to attack an outer space asset. While this issue can be addressed in outer space legislation directly,[217] it would appear more viable that protection of space assets is

[213] Global Commission on the Stability of Cyber Space, *supra* note 29 at 30.
[214] US, "vulnerabilities equities policy and process for the United States Government" at 1 (November 15, 2017) online (pdf): <https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF>
[215] PriceWaterhouseCoopers, *supra* note 98 at [3].
[216] UNODC, *supra* note 2
[217] For example, New Zealand, Outer Space and High-altitude Activities Act (2017), s72

grouped under wider national infrastructure.[218] While the concept of making it illegal to attack a State asset would appear so straightforward (and universally applied) that it hardly needs mentioning, there are a number of additional layers of protection which can usefully be brought into legislation. Another important step in protecting outer space assets from attack, for instance, involves increasing the transparency of the ownership and operational control of such infrastructure. In addition to this, the risks of such an asset being attacked can be mitigated by facilitating cooperation and collaboration between all levels of government, and between regulators, owners and operators of such infrastructure.[219]

States have also passed specific legislation to combat the risks of terrorism outlined in [*Part I(A)(2)(c)*]. This legislation ensures that attempted or actual terrorist attacks against key pieces of infrastructure are treated with a manifest degree of gravity, and ensures that both investigation and prosecution are significantly more severe. The New Zealand Terrorism Suppression Act 2002[220] is a good example of such legislation, defining a 'terrorist act' as being any "serious interference with, or serious disruption to, an infrastructure facility,[221] if likely to endanger human life." This Act does not limit the means by which an attack can take place, and can openly apply to outer space assets.[222] Further, the Act applies widely, having a section for extraterritorial jurisdiction and extradition built into the domestic legislation.

9. Summary

While national approaches to criminalization of cyber-crime tend to be fairly consistent throughout States, their approaches to cyber-crime investigative powers show less core

[218] For example, EUR-Lex, DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (6 Jul 2016) online: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC>
[219] Australia, Security of Critical Infrastructure Act (2018), div 3
[220] New Zealand, Terrorism Suppression Act 2002, s4
[221] Under this act, infrastructure facility means a facility (whether publicly or privately owned) providing or distributing basic services for a population (for example, water, sewage disposal, energy, fuel, or communications)
[222] New Zealand, Terrorism Suppression Act 2002, s4

commonality.[223] Generally, across States it would appear that there needs to be an increase in powers for search and seizure, powers for obtaining stored computer data, powers for real-time collection of data, and powers for ensuring expedited preservation of data.[224]

This recognition is particularly important given that less than half of all States have perceived their criminal and procedural law frameworks to be sufficient.[225] Among those States who report having insufficient laws, only half have indicated that they have plans for new laws, thus highlighting an urgent need for legislative strengthening and capacity building.[226] Further, it is becoming increasingly clear that States tendency to focus on criminalization is proving to be insufficient, perhaps indicating that a shift towards broader legislation which addresses investigative measures, jurisdiction, internet service provider responsibility and liability, and international cooperation is (or should be) on the horizon.[227]

At this stage, there is a lack of consistency of cyber policy between States, which demonstrates the role which international law can play in harmonizing policy and capacity building. In line with this, Part III of this thesis will provide an overview of the international *lex lata* relating to outer space assets and cyber-attacks.

PART III

INTERNATIONAL LAW: THE *LEX LATA*

Considering that all State's outer space assets operate utilizing a shared, single cyberspace, one would envisage that the collective management of the threats posed in this environment would be a priority for all.[228] As will be seen from the analysis below, however, it would appear that international legislation in this area is particularly lacking, with between

[223] UNODC Study on Cybercrime, *supra* note 24 at 133-134.
[224] *Ibid.*
[225] *Ibid* at xvii.
[226] *Ibid.*
[227] *Ibid* at 42.
[228] HM Government, *supra* note *77* at 63.

one-third to one-half of States reporting insufficient frameworks for the criminalization and prosecution of extraterritorial cyber-crime acts.[229]

With that said, there are valuable lessons we can learn from those initiatives which currently exist, on a bilateral, regional and international level. This Part will focus on a variety of examples of *lex specialis* (in regards to outer space and cyberspace) and of *lex generalis*, in a bid to determine what international law currently stands in place to mitigate the threats of cyber security to outer space assets across different groupings of States, and then utilize this information to determine, in Part IV, how international dialogue, policy and cooperation can be better leveraged to mitigate the risk that cyber-attacks pose to outer space assets.

It is also important to note that the phrases 'binding' and non-binding' are used extensively in this Part. Generally, "binding" is defined as creating an obligation, requiring States to act in a certain way, lest they face repercussions. The latter term, "non-binding," tends to *urge* States to act in a certain way on the basis of mutual cooperation.[230] Non-binding law carries more than mere political or moral value, however, given its ability to significantly influence States' behavior and directly contribute to the progressive elaboration and consolidation of international law norms.[231]

A. Bilateral Agreements

By a significant margin, the easiest agreements to make are those that are negotiated bilaterally. The difficulty of coming to a consensus in any agreement multiplies as one adds more States into a negotiation, and keeping the number of parties to a minimum allows States to tailor their agreements more specifically to each State's national circumstances, and to reach

[229] UNODC Study on Cybercrime, *supra* note 24 at xxiv.
[230] B Havel, G Sanchez "The Principles and Practice of International Aviation Law" (2014) Cambridge University Press, New York, at 11
[231] Fabio Tronchetti, "Legal aspects of the military uses of outer space," in Frans von der Dunk Fabio Tronchetti, eds, Handbook of Space Law, (Cheltenham, UK: Edward Elgar, 2015) at 378

an agreement quickly (relatively speaking).[232] While the details of many of these bilateral security discussions are often confidential between States, broad details are sometimes made available to the public.

The following is not intended to be an exhaustive list of bilateral initiatives related to cyber security and the protection of critical assets, nor will it seek to outline every publicly available provision located in the agreements themselves. Instead, it aims to provide an overview of some of the more novel and effective provisions which are in place to curb the risk of cyber-attacks to critical assets, particularly in bilateral dialogues and initiatives associated with military and economic superpowers including United States, Russia, India and China.

1. US-Russia

In 2013, the US and Russia progressed with negotiations on cyber issues, going so far as to establish a standing working group on these issues. The bilateral negotiations also produced a series of transparency and confidence building measures (TCBMs), including those which:[233]

i. Facilitated the exchange of technical information (i.e. malware or malicious indicators) between the US Computer Emergency Response Team and its Russian counterpart;

ii. Expanded the role of the Nuclear Risk Reduction Centre which was established in 1987 to exchange information about planned cyber exercises and for formal inquiries about "cybersecurity incidents of national concern"; and

[232] J Kagan, Bilateral Trade (Investopedia, May 24 2019) online: <https://www.investopedia.com/terms/b/bilateral-trade.asp>

[233] US, Office of the Press Secretary, "Fact Sheet: U.S.-Russian Cooperation on Information and Communications Technology Security", (17 June 2013) online: <https://www.whitehouse.gov/the-press-office/2013/06/17/fact-sheet-us-russian-cooperationinformation-and-communications-technol.>; as per Global Commission on the Stability of Cyber Space, *supra* note 29 at 24.

iii. Established a hotline in the existing Direct Secure Communication System between the White House and the Kremlin to manage any cyber related crisis which might arise.[234]

Such TCBMs play an important role in building relationships and mitigating the threat of cyber-attacks, proving essential tools in State's bids to reduce mistrust, miscalculation and misunderstandings between parties, ultimately reducing the risk of escalation.

2. US-China

In 2015, the US and China also engaged in negotiations on cybersecurity issues, in which Presidents Obama and Xi agreed that "neither country's government [would] conduct or knowingly support cyber enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors."[235]

This agreement was further consolidated into a binding bilateral accord, in which both States pledged not to commit or support economic cyberespionage. This accord also established an experts group to discuss cyber norms, and a ministerial-level group that meets biannually to "review the timeliness and quality of responses to requests for information or assistance with respect to malicious cyber activity."[236] Arguably one of the most important functions of this bilateral accord, however, is the TCBMs which it established, requiring the States to:[237]

i. Exchange assistance in regards to malicious cyber activities;

ii. Answer requests for information from the other State in a timely fashion; and

---

[234] US, *supra* note 233.
[235] Marie Baezner, "Cybersecurity in Sino-American Relations" (Center for Security Studies, No. 224, April 2018) online (pdf): <https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse224-EN.pdf>
[236] *Ibid.*
[237] Two more general Memoranda of Understanding on TCBMs in the field of military relations were signed between China and the US in November 2014. US, Office of the Press Secretary, Fact Sheet: President Xi Jinping's State Visit to the United States, (25 September 2015) online: <https://www.whitehouse.gov/the-press-office/2015/09/25/factsheet-president-xi-jinpings-state-visit-united-states>

iii. Establish a hotline between the two States in case of escalation.[238]

What was particularly notable with regards to this bilateral agreement is that, after it was agreed to, US private sector cybersecurity firms report that the level of Chinese cyber activity against private sector targets in the US has markedly declined.[239]

3. US-India framework document

In 2016, the US and India agreed to a framework document[240] under which both States agreed, for five years, to cooperate on a range of measures such as "law enforcement efforts against cyber-crime", "exchanging cybersecurity best practices", and "promoting specific cyber norms recommended by the UN GGE[241] and the G20."[242] They also agreed to designate a point of contact for each specific area of cooperation outlined in the framework, so as to better facilitate its implementation.

4. US-EU Privacy Shield programs

While it is not a "bilateral agreement" in a sense that one would traditionally imagine, more than 5000 companies are now actively certified under the US-EU Privacy Shield Framework. Finalised in 2016 and administered by the International Trade Administration within the US Department of Commerce, this initiative is a certification mechanism program which facilitates the safe transfer of personal data from the EU to the US in accordance with the EU's General Data Protection Regulation in support of transatlantic commerce.[243] It does

[238] *Ibid*.; Global Commission on the Stability of Cyber Space, *supra* note 29 at 25.
[239] Adam Segal, "The U.S.-China Cyber Espionage Deal One Year Later," Net Politics (blog), the Council on Foreign Relations (2016) online: <https://www.cfr.org/blog/us-china-cyber espionage-deal-one-year-later>; as per Global Commission on the Stability of Cyber Space, *supra* note 29 at 25.
[240] US, Office of the Press Secretary, "Joint Statement: 2016 United States-India Cyber Dialogue" (September 29, 2016) online: < https://obamawhitehouse.archives.gov/the-press-office/2016/09/29/joint-statement-2016-united-states-india-cyber dialogue>.
[241] This refers to the Group of Governmental Experts on Developments in the Field of Information and Communications Technologies in the Context of International Security (GGE:DFICT)
[242] Global Commission on the Stability of Cyber Space, *supra* note 29 at 26.
[243] US Department of Commerce, "EU-U.S. PRIVACY SHIELD FRAMEWORK PRINCIPLES ISSUED BY THE U.S. DEPARTMENT OF COMMERCE" at 1-2 (accessed 19 November 2019) online: <https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004qAg>

this by requiring companies to make public and legally enforceable commitments to comply with the Shield's data protection principles,[244] obligating them to *(not exhaustive)*:

i. Offer individuals the choice of how their personal information is to be handled;[245]

ii. Ensure suitable cyber security protocols in any organization to whom that information is transferred on to;[246]

iii. In cases where an Organization is handling personal information, they must take reasonable and appropriate measures to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction;[247]

iv. Organizations must, in circumstances where they hold individual's personal information, allow those individuals to access that information, and allow them to correct, amend, or delete that information where it is inaccurate.[248]

In addition to providing obligations, this US-EU Privacy Shield establishes processes for monitoring the functioning of the privacy shield, ensuring transparency between States, and developing means for redress in the event of a breach.[249] This framework, then, is revolutionary in that it protects individual's rights, and also gives them direct access to justice across borders – a luxury which they are not normally afforded in international law (which is generally reserved for State-to-State actions only).[250] Such an innovative approach could prove vital to protecting the growing number of private aerospace and satellite manufacturers, in the absence

[244] Privacy Shield framework, "Privacy Shield Overview" (accessed 16 September 2019) online: <https://www.privacyshield.gov/Program-Overview>
[245] Privacy Shield framework, "Articles: 2. CHOICE" (accessed 19 November 2019) online: <https://www.privacyshield.gov/article?id=2-CHOICE>
[246] Privacy Shield framework, "Articles: 3. ACCOUNTABILITY FOR ONWARD TRANSFER" (accessed 19 November 2019) online: <https://www.privacyshield.gov/article?id=3-ACCOUNTABILITY-FOR-ONWARD-TRANSFER>
[247] Privacy Shield framework, "Articles: 4. SECURITY" (accessed 19 November 2019) online: <https://www.privacyshield.gov/article?id=4-SECURITY>
[248] Privacy Shield framework, "Articles: 6. ACCESS" (accessed 19 November 2019) online: <https://www.privacyshield.gov/article?id=6-ACCESS>
[249] European Commission "EU-U.S. Privacy Shield" July, 2016, online (pdf): <https://ec.europa.eu/info/sites/info/files/factsheet_eu-us_privacy_shield_en.pdf>
[250] Ian Brownlie, Principles of Public International Law, at 503 (7th ed., 2008)

of other international agreements, particularly if States pursue international policy to facilitate private sector civil action across borders (as will be discussed further at [*Part IV(B)(16)*].

5. Russia-China

In 2015, Russia and China signed a bilateral agreement in which both States are prohibited from conducting cyber operations against each other.[251] In addition to this general prohibition, Russia and China also committed to engage in regular bilateral dialogues in which they would exchange information and forge cooperation on the creation and dissemination of cyber norms.[252] They further agreed to jointly respond to technologies which they feel may have a destabilising effect on political and socio-economic life, or which may interfere with the internal affairs of either State.[253]

Following from this bilateral agreement, in 2016 Russia and China issued a joint statement which identified each side's respective points of contact, and identified the States' respective efforts to jointly filter information online.[254] While the Russia-China pact is a traditional form of alliance (as seen through bilateral agreements for thousands of years and even the UN Security Council), this agreement to work together on cyber issues could be a huge asset to both States, particularly as both are at the forefront of the cyber and space races.

Russia and China have also, in several circumstances, agreed to join forces to combat cyber issues, making the most of their collective technological advancement and resources.[255] This type of coordination and maximisation of each State's respective technological fortes

[251] Elaine Korzak, "The Next Level for Russia-China Cyberspace Cooperation?" Net Politics (blog), the Council on Foreign Relations (August 20, 2016) online: <https://www.cfr.org/blog/next-level-russia-china-cyberspace-cooperation>; as per Global Commission on the Stability of Cyber Space, *supra* note 29 at 25.
[252] *Ibid.*
[253] Andrew Roth, "Russia and China Sign Cooperation Pacts" (New York Times, May 8, 2015) online: <https://www.nytimes.com/2015/05/09/world/europe/russia-and-china-sign-cooperation-pacts.html>
[254] A Soldatov, I Borogan, "Putin brings China's Great Firewall to Russia in cybersecurity pact," (The Guardian, November 29, 2016) online: <https://www.theguardian.com/world/2016/nov/29/putin-china-internet-great-firewall-russia-cybersecurity-pact>
[255] Global Commission on the Stability of Cyber Space, *supra* note 29 at 25.

could provide a useful template for other States in future attempts to mitigate the risks that cyber-attacks pose to outer space assets.

Russia is also believed to have signed similar agreements with India and South Africa in 2016 and 2017, respectively, although the details of these texts have not been made public.[256]

B. Regional initiatives and organizations

Regional measures tend to be powerful tools for change, owing to their advantage in involving a small number of States[257] with closely related interests, in addition to the fact that they can often build upon highly-developed cooperative arrangements and mature existing institutions.[258] A selection of initiatives and organizations arising from such regional cooperation will be discussed below, particularly as they relate to cyber security[259].

1. European Union

The EU has, since its formation, consistently demonstrated how a series of States with competing interests can come together as a region to resolve issues, and that cooperation continues in the era of cyber threats. Since the 2008 European Council Report on Implementation of the European Security Strategy, which included cyber threats as a new risk to European security,[260] Europe has placed a significant emphasis on cyber security.

The EU is particularly active in two overlapping cyber security areas, both of which play a significant role in the current issue of mitigating the risks which cyberattacks pose to outer space assets: measures to combat cyberattacks including cyber-crime, and measures to support critical infrastructure protection and network security.[261]

---

[256] Arun Mohan Sukumar, "India and Russia sign cyber agreement, pushing the frontier for strategic cooperation," (Observer Research Foundation, October 15, 2016) online: <https://www.orfonline.org/expert-speak/india-and-russia-cyber agreement/>; as per Global Commission on the Stability of Cyber Space, *supra* note 29 at 25.
[257] Relative to multilateral agreements.
[258] J Lewis, G Neuneck, *supra* note 23 at 101.
[259] As prevalent regional agreements which relate to the security of outer space assets, at this stage, do not exist.
[260] European Council, Report on Implementation of the European Security Strategy: Providing Security in a Changing World, (11 December 2008) EU document S407/08.
[261] J Lewis, G Neuneck, *supra* note 23 at 104.

a) Binding Initiatives

Making the most of its unique governance structure, the EU has been able to pass a number of binding initiatives which, were it not for this governance arrangement, could perhaps have been too difficult to organize between 28 separate member States.

One such example is the European Council Directive on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.[262] This policy is interesting in that it lists "digital infrastructure" together with other well-recognised pieces of national critical infrastructures (such as water supply and transportation), thus representing a well-deliberated policy decision by EU Member States to use the existing resilience network to protect cyber space.[263] This directive is also important as it marked the first time that a major global economic body decided to take the critical infrastructure protection route for securing internet operation, recognizing the internet's protocols and key services as a part of civilian critical infrastructure protection.[264] While outer space assets have themselves not been considered critical infrastructures,[265] as these assets either directly or indirectly manage all of those infrastructures which are listed (including in the categories of energy, transport, banking, health sector and digital infrastructure) they could plausibly be considered as such.

It is also instructive to discuss the EU Directive 2016/1148 which, among other things, mandated the reporting of cyber incidents.[266] While this reporting provision was later dropped,[267] this exercise provided useful dialogue, demonstrating that the issue of information

[262] 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
[263] Global Commission on the Stability of Cyber Space, *supra* note 29 at 87.
[264] *Ibid.*
[265] Defined in the Tallinn Manual as all systems and assets, physical and virtual, within a nation state's jurisdiction that "are so vital that their incapacitation or destruction may debilitate a State's security, economy, public health or safety or the environment"; Tallinn Manual 2.0, *supra* note 17 at 258.
[266] EUR-Lex, *supra* note 218 at (2)
[267] *Ibid* at (4).

sharing, as discussed at [*Part II(B)(6)*], is at the forefront of States' agendas (even if it proved unmanageable for the time being).

b) Non-Binding Initiatives

The Organization for Security Co-operation in Europe (OSCE) was established in 2008 and is made up of 57 States located across Europe, North America, and Asia. It offers a regional forum for high-level dialogue with a comprehensive view on security, combining politico-military, economic, environmental, and human dimensions.[268] It is the largest security-oriented regional intergovernmental organization, covering most of the northern hemisphere, and a wide range of topics.[269]

The OSCE first addressed cyber security concerns in the OSCE declarations and resolutions, which were adopted in 2008 in Astana, Kazakhstan[270] calling on the international community "to increase cooperation and information exchange in the field of cyber security, to agree on specific measures to counter the cyber threat and to create, where possible, universal rules of conduct in cyberspace."[271] The OSCE also places significant emphasis on States developing vulnerability disclosure policies, wherein State security agencies discover and publish details of computer vulnerabilities, thereby by signalling to others that they are not stockpiling computer flaws for future use, and improving the stability of cyber space.[272]

---

[268] OSCE "What we do" (Accessed 5 December 2019) online: <https://www.osce.org/what-we-do>
[269] A Sternstein, "Cyber early warning deal collapses after Russia balks" (NextGov, 7 December 2012) online: <https://www.nextgov.com/cybersecurity/2012/12/cyber early-warning-deal-collapses-after-russia-balks/60035/>
[270] OSCE, Astana Declaration of the OSCE Parliamentary Assembly and Resolution Adopted at the Seventeenth Annual Session (Organization for Security and Co-operation in Europe, Seventeenth Annual Session, Astana, 29 June to 3 July 2008) online (pdf): <https:// ccdcoe.org/sites/default/files/documents/OSCE-080703-AstanaDeclarationandResolutions.pdf> A Osula, H Roigas "International Cyber Norms: Legal, Policy & Industry Perspectives" at 1377 (CCDCOE, 2016) online (pdf): <https://ccdcoe.org/uploads/2018/10/InternationalCyberNorms_full_book.pdf>
[271] OSCE, Belgrade Declaration of the OSCE Parliamentary Assembly and Resolution Adopted at the Twentieth Annual Session (Organization for Security and Co-operation in Europe, Twentieth Annual Session, Belgrade, 6-10 July 2011) online (pdf): <https://www. oscepa.org/documents/all-documents/annual-sessions/2011-belgrade/declaration-4/3024-belgrade-declaration-eng/file>; as per A Osula, H Roigas, *supra* note 270 at 1377.
[272] Alex Grigsby, "Disclosing Policies on Zero-Days as a Confidence-Building Measure," Net Politics (Council on Foreign Relations, November 18, 2014) online: <https://www.cfr.org/blog/disclosing-policies-zero-days-confidence-buildingmeasure>

Further, and particularly relevant to the current discussion, in 2012 the OSCE began developing the first set of TCBMs to enhance inter-State co-operation, transparency, predictability, and stability, and to reduce the risks of misperception, escalation, and conflict that may stem from the use of cyber technologies.[273] These TCBMs focused on a variety of target areas, asking States to undertake a number of measures including providing a list of national terminology and definitions related to ICT security, and suggesting implementation of measures to facilitate cross-border cooperation to fight cyber-crime and terrorist use of ICTs.[274] The OSCE further adopted a second set of TCBMs in 2016,[275] though these received a poor international reception and have been deemed as not particularly useful.[276]

2. Asia

As a diverse and highly populated region, Asia has started a number of important initiatives relating to cyber security and the protection of national infrastructure – primarily through regional organizations.

The ASEAN regional forum (ARF) is particularly important in this regard. Founded in 1994 and consisting of 27 participating States, the ARF is active in discussing and implementing TCBMs and preventative diplomacy.[277] In 2006, the ARF issued the "ARF Statement on Cooperation in Fighting Cyber-attack and Terrorist Misuse of Cyber Space."[278] This statement was particularly important as the focus on terrorism in cyberspace is a critical and often underdiscussed issue (as discussed at [*Part I(A)(2)(c)*]). Expanding upon this work,

[273] OSCE, Permanent Council decision No. 1039, Development of Confidence Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies, PC.DEC/1039 (26 April 2012) online: <http://www.osce.org/pc/90169?download=true>
[274] J Lewis, G Neuneck, *supra* note 23 at 133.
[275] OSCE 2016 set of CBMs, Decision No 1202
[276] CCDCOE, *supra* note 164 at 2.
[277] ASEAN Regional Forum, "About the ASEAN Regional Forum" online: <http://aseanregionalforum.asean.org/about.html>
[278] Ministry of Foreign Affairs of Japan "ASEAN REGIONAL FORUM STATEMENT ON COOPERATION IN FIGHTING CYBER-ATTACK AND TERRORIST MISUSE OF CYBER SPACE" (Kuala Lumpur, 28 July 2006) online: <https://www.mofa.go.jp/region/asia-paci/asean/conference/arf/state0607-3.html>

in 2012 the ARF held the "Workshop on Proxy Actors in Cyber Space" which outlined best practices for implementing agreed guidelines, and designated a forum for the discussion of TCBMs in cyberspace.[279]

Separately but equally important, we must discuss the Shanghai Cooperation Organization (SCO). This organization, founded in 2001, encompasses approximately 60% of the Eurasian land mass[280] and was established for the purposes of addressing political, economic and military organization.[281]

In 2011, the SCO published their "Agreement on Cooperation in the Field of Information Security",[282] which outlines the threat of "the development and use of information weapons, preparing and waging information war" and the "use of [a] dominant position in the information space to the detriment of the interests and security of other States."[283] This Agreement has played an important role in bringing a range of new issues to the forefront of attention at an international level, not least of which is its urging of States to refrain from inducing their private sector actors to introduce backdoors (ie. deliberate zero-day malware) into their hardware or software.[284]

The SCO has since played a key role in the development of international cyber space policy, strongly advocating for a new international instrument to manage the issue of cyber-crime, and also calling on States to agree to not conduct, or knowingly support, activity which intentionally damages critical infrastructure.[285]

---

[279] ARF Workshop on Proxy Actors in Cyberspace, "Co-chairs' summary report" (Hoi An City, Viet Nam, 14–15 March 2012) online: <http://aseanregionalforum>
[280] Made up of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan, and Uzbekistan.
[281] J Lewis, G Neuneck, *supra* note 23 at 103.
[282] Shanghai Cooperation Organization, "Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security" (61st plenary meeting, 2 December 2008) online: <http://media.npr.org/assets/news/2010/09/23/cyber_treaty.pdf>
[283] *Ibid* at annex 2, item 1
[284] Global Commission on the Stability of Cyber Space, *supra* note 29 at 30.
[285] CCDCOE, *supra* note 164 at 4.

3. The Americas

The collective States of the Americas have carried out extensive work in the area of cyber security, notably through the Organization of American States (OAS).

The OAS, established in 1889 and encompassing all 35 independent states of the northern, central, and southern Americas, covers a wide range of security and political issues.[286] The organisation has carried out extensive work to combat the risk of cyber-attacks, including forming a Group of Governmental Experts on Cyber-crime to analyse criminal activities related to computer networks, compare national legislation, and identify national and international entities with relevant expertise.

Following from this work, the Organization's General Assembly approved the Inter-American Integral Strategy to Combat Threats to Cybersecurity,[287] and provided a mandate to the Inter-American Committee against Terrorism (CICTE) to begin working on cybersecurity.

Through the CICTE, the OAS also made notable contributions to capacity-building efforts, training and assisting Latin American countries to develop national cybersecurity strategies and to build their incident response capabilities, and went on to create a cybersecurity programme and establish national Computer Security Incident Response Teams (CSIRTs).[288]

In 2012, the OAS also approved the Declaration on Strengthening Cyber Security in the Americas, which called for the development of national cyber strategies and strengthening international cooperation mechanisms.[289] This work demonstrates a concerted focus on strengthening cyber security across a broad range of threat vectors, and reveals the Americas increasing awareness of the risk that cyber-attacks pose.

---

[286] OAS, "Cyber security program" online: <www.oas.org/en/sms/cyber>
[287] OAS, ADOPTION OF A COMPREHENSIVE INTER-AMERICAN STRATEGY TO COMBAT THREATS TO CYBERSECURITY: A MULTIDIMENSIONAL AND MULTIDISCIPLINARY APPROACH TO CREATING A CULTURE OF CYBERSECURITY (Resolution 2004 XXXIV-O/04, June 8, 2004) online (pdf): <https://www.oas.org/en/sms/cicte/Documents/OAS_AG/AG-RES_2004_(XXXIV-O-04)_EN.pdf>
[288] J Lewis, G Neuneck, *supra* note 23 at 103.
[289] OAS, "Press Release: OAS Presents Mobile Simulation Laboratory for Cyber-attack Response Exercises" (August 31, 2012) online: <http://www.oas.org/en/media_center/press_release.asp?sCodigo=E-298/12>

4. Africa

While States throughout the African region have struggled with implementing consistent cyber-crime policy, the region as a whole has produced a range of both binding[290] and non-binding initiatives.[291] Of particular importance is the draft Economic Community of West African States (ECOWAS) Directive on Fighting Cyber-crime (2009),[292] which, among other things, notably mandated the criminalization of illicitly 'remaining' in a computer system after authorization to be in that system has lapsed (as previously discussed at [*Part II(B)(2)*]).[293] Additionally, the non-binding Common Market for Eastern and Southern Africa (COMESA) Cybersecurity Draft Model Bill (2011)[294] provides a comprehensive outline of laws which could be implemented to combat cyber-crimes, covering in detail such topics such as jurisdiction, extradition, providing assistance to other State parties, and best practices on gathering stored data for evidential purposes.

5. League of Arab States

The League of Arab States was established in 1945 and comprises 22 Members. Regionally, the League has been quite active in cyber-crime policy, engaging with and hosting widely on issues of cyber-crime in the international community, including the Arab Security Conference.[295]

---

[290] For example, the Draft African Union Convention on the Establishment of a Legal Framework Conducive to Cybersecurity in Africa (2012)
[291] For example, the East African Community Draft Legal Framework for Cyberlaws (2008), and the Southern African Development Community (SADC) Model Law on Computer Crime and Cyber-crime (2012)
[292] Economic Community of West African States "Harmonization of ICT Policies in Sub-Saharan Africa" at art. 3(ITU, 2013) online (pdf): <https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/cyber-crime_directive-explanatory_notice.pdf>
[293] UNODC Study on Cybercrime, *supra* note 24 at 85.
[294] Common Market for Eastern and Southern Africa, COMESA Draft Model Bill (Gazette Vol 16, 2011) online (pdf): <https://www.comesa.int/wp-content/uploads/2016/06/2011Gazette-Vol.-16.pdf> [COMESA Draft Model Bill]
[295] International Democracy Watch, League of Arab States (accessed 05 December 2019) online: <http://www.internationaldemocracywatch.org/index.php/monitored-igos/interregional-organisations/568-league-of-arab-states>

Notably, the League also created the extremely comprehensive League of Arab States Convention on Combating Information Technology Offences (2010),[296] which mandates provisions for obtaining stored data, provides a template for a range of criminal acts, and includes model provisions for both jurisdiction and extradition.

6. The Commonwealth

The most significant cyber-crime initiative to come out of the commonwealth is the 2002 Commonwealth Model Laws on Computer and Computer-related Crime and Electronic Evidence. These model laws were designed with the purpose of supporting Commonwealth countries to put in place a legal framework for criminalisation and investigation of computer and computer-related crimes.[297]

The banning of computer misuse tools (as discussed at [*Part II(B)(2)*]) is a particularly innovative addition to these model laws, with States being urged to mandate that any person commits an offence who "intentionally or recklessly, without lawful excuse or justification, produces, sells, procures for use, imports, exports, distributes or otherwise makes available… a device, including a computer program, that is designed or adapted for the purpose of committing an offence…"[298] These are also innovative in that they cover crimes directed at computers and ICTs, such as unauthorised access and distributed denial of service attacks.[299]

[296] League of Arab States, Arab Convention on Combating Technology Offences (21 Dec, 2010) online: <https://dig.watch/instruments/arab-convention-combating-technology-offences>
[297] Commonwealth Office of Civil and Criminal Justice Reform, Model Law on Computer and Computer Related Crime, Introduction (Commonwealth Secretariat, 2017) online (pdf): <http://thecommonwealth.org/sites/default/files/key_reform_pdfs/P15370_11_ROL_Model_Law_Computer_Related_Crime.pdf> [Commonwealth Model Laws]
[298] *Ibid* at 9(1)
[299] Australia, *supra* note *147* at 22.

The efficacy of these model laws is evident when considering that the UK's Criminal Code Act 1995[300] and the Telecommunications (Interception and Access) Act 1979,[301] were directly based upon these templates.

7. The North Atlantic Treaty Organization (NATO)

The North Atlantic Treaty Organization (NATO) is an intergovernmental military alliance between 29 North American and European countries and is the largest military alliance in the world, whose mandate is restricted to collective defence and crisis management in the North Atlantic area.[302]

NATO started its cyber defence programme in 2002, following the denial-of-service attacks carried out during the Kosovo war.[303] As an extension of this work, in 2008 the Cooperative Cyber Defence Centre of Excellence (CCDCOE) was established in Tallinn, Estonia, to conduct research, education, and training and to host workshops on legal, doctrinal, and technical cyberwarfare issues (the highly esteemed 'Tallinn Manual' and its associated articles flow from this).[304] NATO's approach to cyber stability is now one of norms and deterrence, carried out through the public signalling of rules which NATO determined to be applicable to cyber space.[305]

In 2014, NATO agreed that international law applied to cyber space, and agreed also that an offensive cyber operation against it could trigger the collective self-defence provision under Article 5 of the Organization's Convention.[306]

---

[300] Commonwealth Consolidated Acts, Criminal Code Act 1995, online: <http://www5.austlii.edu.au/au/legis/cth/consol_act/cca1995115/sch1.html>
[301] Telecommunications (Interception and Access) Act 1979, online: <http://classic.austlii.edu.au/au/legis/cth/consol_act/taaa1979410/>
[302] NATO Cooperative Cyber Defence Centre of Excellence, "About" (accessed 02 December 2019) online: <www. ccdcoe.org>
[303] For details see, S. Myrli, NATO and Cyber Defence, para 45 (NATO, 173 DSCFC 09 E bis, 2009).
[304] NATO Cooperative Cyber Defence Centre of Excellence, "About" (2019) online: <www. ccdcoe.org>
[305] Global Commission on the Stability of Cyber Space, *supra* note 29 at 21.
[306] *Ibid.*

8. Summary

As demonstrated in this section, regional inter-governmental organizations have been extremely useful in building cyber security rules, norms, and capacity. In this vein, it is also particularly important to note the importance of regional instruments and organizations in developing and implementing cooperative security arrangements and TCBMs,[307] as well as in approaching new issues such as cyber terrorism, capacity building, collective self-defence, and collective research.

The degree of harmonization of cyber-crime laws reported by States within a region varies significantly from State to State. In a UNODC study, approximately one third of States reported that their legislation was either 'very highly' or 'highly' harmonised with other countries in their region, while the remainder view their legislation as 'partially' or 'somewhat' harmonised with those States[308] (incidentally, levels of perceived harmonization tend to be higher in Europe and the Americas than in Africa, Asia and Oceania).[309]

The natural next step from regional agreements, is to seek greater harmonization across a larger geographical area: namely, pursue a well-implemented agreement across a larger number of states.

C. Multilateral Agreements

The emerging importance of multilateralism in cyber space and outer space cannot be overstated. Up to 70% of cyber-crime involves a transnational dimension[310] and though details on attacks on outer space assets are thusfar scarce, one would imagine these would generally involve a similar State-to-State dimension. In this regard then, to quickly and efficiently reach a maximum degree of global harmonization, States should ideally seek to obtain as large a number of ratifying parties as possible in any new agreement.

[307] J Lewis, G Neuneck, *supra* note 23 at 101.
[308] UNODC Study on Cybercrime, *supra* note 24 at 59.
[309] *Ibid* at 56.
[310] *Ibid* at xxiv.

In line with this, issues of transnational investigations, sovereignty, jurisdiction, extraterritorial evidence, and a requirement for international cooperation, are particularly important in these environments.

1. Outer Space multilateral policy

Outer Space multilateralism is relatively limited, being made up of five primary, binding United Nations treaties:

i. The 1967 Outer Space Treaty,[311] which entered into force on 10 October 1967. It has been ratified by 109 States, with 23 additional States providing a signature with no ratification,[312] and sets a broad foundation upon which all other outer space treaties are based;

ii. The 1968 Rescue and Return Agreement,[313] which has 98 ratifying parties and expands paragraphs V and VIII of the Outer Space Treaty, mandating the return of all found astronauts and space objects to their State of registry;

iii. The 1972 Liability Convention,[314] which has 96 ratifying parties and expands upon Article VII of the Outer Space Treaty, ensuring that States are held liable for damage which their space objects cause to other space objects;

iv. The 1976 Registration Convention,[315] which has 69 ratifying parties and extrapolates on the notion of registration mentioned in Article V and VIII of the Outer Space Treaty, setting out the requirements for registration of space objects; and

[311] Outer Space Treaty, *supra* note 8.
[312] See Committee on the Peaceful Uses of Outer Space Legal Subcommittee, Status of International Agreements relating to activities in outer space as at 1 January 2019 (A/AC.105/C.2/2019/CRP.3) online: <http://www.unoosa.org/documents/pdf/spacelaw/treatystatus/AC105_C2_2019_CRP03E.pdf>
[313] Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space, Apr. 22, 1968, 672 U.N.T.S 119
[314] Liability Convention, *supra* note 38.
[315] Convention on Registration of Objects Launched into Outer Space, Sept. 15, 1976, 28 U.S.T. 695, 1023 U.N.T.S 15

v. The 1979 Moon Agreement,[316] which has 18 ratifying parties and expands upon various portions of the Outer Space Treaty, particularly relating to peaceful purposes (Article IV) and the appropriation of the moon and celestial bodies (Article II).

Among these instruments, the most applicable to the issue of cyber-attacks on outer space assets is the Outer Space Treaty, as a result of its broad commitments. In addition to these treaties, the thesis will also consider the work done by the International Telecommunication Union (ITU)

a) 1967 Outer Space Treaty

Article III of the Outer Space Treaty provides that 'activities in the exploration and use of outer space' shall be carried out 'in accordance with international law, including the Charter of the United Nations, in the interest of maintaining international peace and security'.[317] This is particularly important, as it makes room to apply more general areas of law to outer space, as discussed later at [*Part III(C)(3)*]. In addition to this general inclusion of international law in the outer space environment, it has also been posited that any cyber operation involving outer space which threatens international peace and security can be said to violate the general prohibition of activities in outer space that are not for peaceful purposes (outlined in the preamble to the treaty), even if they do not violate other rules of international law.[318]

Besides these generally vague provisions, however, this treaty provides no explicit prohibition against launching attacks against outer space assets, cyber or otherwise.

[316] Agreement Governing the Activities of States on the Moon and Other Celestial Bodies, Dec. 5, 1979, 1363 U.N.T.S.
[317] Outer Space Treaty, *supra* note 8 at Art. 3.
[318] Tallinn Manual 2.0, *supra* note *17* at 276.

b) The Constitution and Convention of the International Telecommunication Union

The ITU is a specialised United Nations agency for regulating telecommunications and the use of the radio frequency spectrum. In line with this, the *raison d'être* of the ITU is to prevent interference in the use of radio frequency spectrum via the allocation and assignment of segments of the spectrum to different services. The ITU's founding Convention, the ITU Constitution and Convention, while not specifically an outer space Treaty, is the governing document for all radio frequencies relating to outer space assets (which are used for ground-to-satellite communication) and is thus considered foundational for outer space activities.

Further to this outer space focus, the ITU has been instrumental in the fight against cyber-crime. As an example, in 2007 an ITU High-Level Expert Group on Cybersecurity was established as a consultation platform for information security experts from various domains and regions[319] in order to "provide a framework within which all stakeholders can coordinate an international response to the growing challenges in cybersecurity" and "to build confidence and security in the information society."[320] Their focus was divided into five primary areas: legal measures, technical procedures, organizational structures, capacity-building, and international cooperation.[321]

It is also important to note that, in accordance with the Plenipotentiary Conference of the International Telecommunications Union in Dubai in 2018, the ITU resolved to focus on "resources and programmes on those national, regional and international areas of cybersecurity within its core mandate and expertise, notably the technical and development spheres, and not including areas related to Member States' application of legal or policy principles related to

[319] J Lewis, G Neuneck, *supra* note 23 at 96.
[320] H.I. Touré, "The Quest for Cyberpeace" at 104 (ITU and World Federation of Scientists, 2011) online (pdf): <https://citizenlab.org/cybernorms2012/cyber peace-itu.pdf>
[321] ITU, Global Cybersecurity Agenda (GCA) (accessed 19 September 2019) online (pdf): <www.itu.int/osg/csd/cybersecurity/gca/new-gca-brochure.pdf>

national defence, national security, content and cyber-crime, which are within their sovereign rights."[322]

The ITU has carried out tremendous work with regards to collating data, and forming policy relating to cyber security, releasing a wide range of quality deliverables (those mentioned above, as well as throughout this thesis, such as the Global Cybersecurity Index[323] and the 2012 ITU/CARICOM/CTU policy guidelines[324] are key examples). The focus of the ITU, however, rests in norm-setting and capacity building regarding outer space and cyberspace, as opposed to creating any obligations on States to refrain from attacking outer space assets. As such, the work of the ITU does not provide any strict control over undesirable State actions.

c) Summary

While it has been argued that, given the unique nature of the outer space environment, outer space treaties would form *lex specialis* on any matters related to outer space and thereby prevail over contrary rules considered in cyber space regulations,[325] the generally flimsy nature of these treaties in terms of binding prohibitions against cyber-attacks makes it appropriate to look beyond the treaties for other ways in which space assets can be protected.

2. Cyber Space multilateral policy

Surprisingly, for as often as cyber security is broached on a domestic and regional level, there are very few binding multilateral treaties which seek to mandate rules surrounding cyber threats. The one exception is the 2001 Budapest Convention on Cyber-crime[326] though, as outlined below, this too has some key limitations.

---

[322] ITU, Collection of the basic texts adopted by the Plenipotentiary Conference, at 523 (ITU Publications, 2019) online (pdf): <http://search.itu.int/history/HistoryDigitalCollectionDocLibrary/5.22.61.en.100.pdf>
[323] ITU, *supra* note 141.
[324] ITU/CARICOM/CTU Model Legislative Texts, *supra* note 144.
[325] Tallinn Manual 2.0, *supra* note 17 at 272.
[326] Budapest Convention, *supra* note *12*.

a) 2001 Budapest Convention on Cyber-crime

The Budapest Convention (otherwise known as the 'Convention on Cyber-crime'),[327] forged by the member-states of the Council of Europe as well as Canada, Japan, South Africa and the US,[328] entered into force in 2004 and currently has 62 State parties, with a further 10 States being signatories or having been invited to accede.[329] The Budapest Convention is the only internationally binding multilateral treaty on cyber-crime,[330] and perhaps the most used multilateral instrument for the development of cyber-crime legislation in the world, covering a wide range of issues in both the public and private sectors.[331]

In addition to setting out general principles for international cooperation on cyber-crime (particularly between internet service providers and law enforcement agencies),[332] this Convention takes important steps in mandating the adoption of legislation to criminalize certain actions (such as illegal access, illegal interception, data interference, system interference, misuse of devices etc. and search and seizure of stored data (art. 2-6, 19-20)), and requires States to enact legislation which defines jurisdiction for such offences (art 22). Further, it mandates that parties to the treaty co-operate with each other on criminal matters related to the treaty, and allows for extradition in the case of transnational crime (art. 23-24). This Convention is also backed up by capacity-building programmes, which were established by the Council of Europe and which focus on law enforcement and judicial training, strengthening of legislation, and establishment of specialised institutions.[333]

---

[327] The Council of Europe (not to be confused with the European Council or the Council of the European Union) is not a body of the European Union but instead an intergovernmental organisation. It has no legislative power, but instead enforces agreements made by European states, through arms such as the European Court of Human Rights. As per L Johnstone, Euronews answers: The Council of Europe turns 70, but what does it do? (euronews, 02 October, 2019) <https://www.euronews.com/2019/10/01/euronews-answers-the-council-of-europe-turns-70-but-what-does-it-do>
[328] A Seger, *supra* note 13.
[329] CCDCOE, *supra* note 164 at 3.
[330] J Lewis, G Neuneck, *supra* note 23 at 99.
[331] UNODC Study on Cybercrime, *supra* note 24 at xxiv.
[332] J Lewis, G Neuneck, *supra* note 23 at 99.
[333] A Seger, *supra* note 13.

The US is one of the most significant proponents of the Budapest Convention, lauding its efficacy as effective mechanism for enhancing international cooperation in cyber-crime cases. In line with this, the US has encouraged accession, stating that State-to-State cooperation and assistance when investigating and prosecuting cyber-crime cases is most effective when the countries have common cyber-crime laws that facilitate evidence-sharing, extradition, and other types of coordination.[334] This Convention is clearly the most ambitious effort to provide a united and robust scheme of cyber security and cooperation and could, on the face of it, be a significant asset in helping to mitigate the risks that cyber-attacks pose to outer space assets (or at least would help to hold perpetrators accountable).

The issue, however, is that at this stage the Convention has only 63 ratifications, with some significant parties missing, such as India, China and Russia (and, as mentioned previously at [*Part I(A)(2)(d)*], these regions are, notably, where the majority of cyber-attacks originate).[335] In addition to issues of Membership, there has also been significant concern expressed by some that, while the Budapest Convention offers a legal basis and a practical framework for police-to-police and judicial cooperation on cyber-crime, this Convention is a criminal justice treaty which does not cover State actors.[336] Russia also notably expressed concern over provisions of the Budapest Convention which, in its view, violate international law norms and countries' sovereignty.[337]

As an alternative to accession to the Budapest Convention, Russia, China, Tajikistan and Uzbekistan opted to send a letter to the UN asking for a resolution on a code of conduct in cyber space, which could include provisions intended to stop terrorists' use of the Internet.[338]

---

[334] US "International Strategy for Cyberspace" at 20 (May 2011) online (pdf): <https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf>
[335] UNODC Study on Cybercrime, *supra* note 24 at 49.
[336] A Seger, *supra* note *13*.
[337] J Kirk, "Despite Controversy, Cyber-crime Treaty Endures" (PCWorld, 21 November 2011) online: <https://www.pcworld.com/article/244407/despite_controversy_cyber-crime_treaty_endures.html>
[338] *Ibid*.

While the Budapest Convention is a significant milestone in international cyber security, the non-participation of a number of significant parties (those mentioned above, as well as essentially all of South America, Asia, Africa and the Middle East) as well as the purported restrictive scope of the Convention severely limit its effectiveness.

b) United Nations Group of Governmental Experts Consensus reports

The Group of Governmental Experts on Developments in the Field of Information and Communications Technologies in the Context of International Security (GGE:DFICT) was first proposed in 2001, and has since met on five occasions. After each of these meetings, the GGE:DFICT attempts to create a non-binding consensus report. The GGE:DFICT is considered to be the UN's most high-profile initiative to improve cyber stability.[339]

The first GGE:DFICT convened in 2002 and consisted of 15 members selected on the basis of an equitable geographical distribution. On this occasion, however, the Group failed to submit a consensus report.

The second meeting of the GGE:DFICT was in 2009. In this circumstance, perhaps spurred on by Estonia and Russia's campaign of cyber activities in their 2008 conflict with Georgia,[340] the GGE:DFICT successfully delivered a summary report. In that report, the Group recommended that States consider norms, confidence building measures, and capacity building initiatives to "reduce the risk of misperception" in cyber space.[341] This report also stressed that 'uncertainty regarding attribution and the absence of common understanding regarding acceptable State behaviour may create the risk of instability and misperception'.[342]

---

[339] Global Commission on the Stability of Cyber Space, *supra* note 29 at 17.
[340] A Henrikson "The end of the road for the UN GGE process: The future regulation of cyberspace" at 2 (Journal of Cybersecurity, Volume 5, Issue 1, 2019) online: <https://academic.oup.com/cybersecurity/article/5/1/tyy009/5298865>
[341] United Nations General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, at 4 (A/65/201 July 30, 2010) online (pdf): <http://www.unidir.org/files/medias/pdfs/final-report-eng-0-189.pdf>
[342] *Ibid*. at 2.

The Group set up a third GGE:DFICT to meet in December 2011, tasked specifically with discussing "norms, rules or principles of responsible behaviour of States."[343] On this occasion, the Group was also able to produce a consensus report which stated, notably, that international law and the Charter of the United Nations apply to State conduct of ICT-related activities.[344] This is particularly important as it relates to the next section of this thesis, the applicability general international law to the issue of cyber-attacks to outer space assets.

In December 2013, a fourth GGE:DFICT was assembled and, in July 2015, that Group submitted a consensus report.[345] This report was significantly more ambitious than the previous two, outlining voluntary peacetime norms for States to follow, and asking States to:[346]

i. Respond to requests for assistance;

ii. Develop vulnerability disclosure policies, disclosing how State security agencies discover computer vulnerabilities and inform vendors.[347]

iii. Not knowingly allow their territory to be used for internationally wrongful cyber acts;

iv. Not conduct or knowingly support activity that intentionally damages critical infrastructure;[348]

v. Not induce private sector actors to introduce backdoors (ie. deliberate zero-day malware) into their hardware or software;[349]

Of major note, this report also focused extensively on reducing tension through the development of TCBMs, and norms of responsible State behaviour,[350] particularly in the sharing of information on national organisations, strategies and programmes, developing focal

[343] UNGA, Developments in the field of information and telecommunications in the context of international security (A/Res/66/24, 2011) online (pdf): <https://undocs.org/A/RES/66/24>
[344] A Henrikson, *supra* note *340* at 3.
[345] See A/Res/68/243 (2013), as per United Nations General Assembly, *supra* note 340 at 5.
[346] Global Commission on the Stability of Cyber Space, *supra* note 29 at 17.
[347] Alex Grigsby, *supra* note *272*.
[348] Global Commission on the Stability of Cyber Space, *supra* note 29 at 35.
[349] *Ibid* at 30.
[350] A Osula, H Roigas, *supra* note 270 at 130.

points for the exchange of information on malicious Information and Communication Technology (ICT) use, and providing assistance to other States in investigations.[351] As a result of these measures, this report is regarded as a significant breakthrough,[352] having developed the most comprehensive set of measures to date.[353]

In June 2017, the fifth (and thus far the last) GGE:DFICT assembled, though the Group failed this time to produce a consensus report. In response to this failure, however, the Group did adopt two new resolutions: one creating a new GGE:DFICT for 2019,[354] and the other creating an open-ended working group (OEWG)[355] to "further develop the rules, norms and principles of responsible behaviour of States", to introduce changes if necessary, and to study the possibility of establishing regular institutional dialogue "with broad participation under the auspices of the United Nations".[356]

The work of the GGE:DFICT is influential, and gives us both cause for hope, as well as a call to despair. As to the former, the GGE:DFICT has reached consensus on so many occasions and provided a wide range of helpful initiatives. As to the latter, the fact that the Group failed to reach consensus in both 2013 and 2017 demonstrates that there is still significant divergence in the circumstances and goals of even the most progressive and aligned parties.

---

[351] A Osula, H Roigas, *supra* note 270 at 139.
[352] United Nations General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security, A/RES/68/243 (9 January 2014) online (pdf): <http://www.unidir.org/files/medias/pdfs/developments-in-thefield-of-information-and-telecommunications-in-the-context-of-international-security-2014-2015-a-res-68-243-eng-0-589.pdf>
[353] A Osula, H Roigas, *supra* note 270 at 136.
[354] United Nations General Assembly, Advancing responsible State behaviour in cyberspace in the context of international security, A/C.1/73/L.37 (11 December 2018) online: <https://undocs.org/A/C.1/73/L.37>
[355] United Nations General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security, A/RES/68/243 (9 January 2014) online (pdf): <http://www.unidir.org/files/medias/pdfs/developments-in-thefield-of-information-and-telecommunications-in-the-context-of-international-security-2014-2015-a-res-68-243-eng-0-589.pdf>
[356] Alex Grigsby, 'The United Nations Doubles Its Workload on Cyber Norms, and Not Everyone Is Pleased', Council on Foreign Relations (November 2018), as per CCDCOE, *supra* note 164 at 2.

c) United Nations Resolution 57/239 – 'Creation of a Global Culture of Cybersecurity'

This non-binding resolution focused on the 'Creation of a Global Culture of Cybersecurity', and worked on the basis that effective cybersecurity is an issue which must be addressed through prevention and supported throughout society, as opposed to a matter of government, law enforcement, or technology alone.[357] As discussed at [*Part II(B)(5)(a)*], this ground-up, societal-centric cyber literacy point of view has been raised through domestic policy a number of times, and such ground level mitigation can help to generate a higher standard of cyber security through both industry and government agencies alike.

d) Summary

Much like outer space, cyber space multilateralism is decisively light. While the Budapest Convention has made notable headway, the non-participation of a number of significant parties, as well as the fact that some States view it as a criminal justice treaty for which the coverage of States is out of scope, severely limits its effectiveness. Given these issues, it is useful to look toward more general areas of international law.

At this point, the lack of any clear prohibition against cyber-attacks to critical assets has resulted in the impunity of perpetrators in numerous instances.[358] While some have resorted to a broad definition of the 'use of force' prohibition under Article 2(4) of the UN Charter to enable prosecution of malicious actors, there is a question as to whether this interpretation is an overly expansive interpretation of that Article.[359] This next section will discuss the merits of that claim and criticism..

[357] United Nations General Assembly, Creation of a Global Culture of CyberSecurity, GA57/239 LVII A/RES/57/239 (2003) online (pdf): <https://www.oecd.org/sti/ieconomy/UN-security-resolution.pdf>
[358] Tzeng, *supra* note 14.
[359] *Ibid.*

3. *Lex Generalis* relating to cyber-attacks on outer space assets

While, as mentioned at [*Part III(C)(2)*], Article III of the Outer Space Treaty[360] clearly states that general international law and the United Nations Charter apply to outer space law, there has also been a significant amount of dialogue surrounding the extent to which general international law applies to cyberspace and cyber-attacks.

Generally, there appears to be broad consensus that international law does apply to cyber space. This position was expressed by NATO in the 2014 Wale Summit Declaration,[361] the GGE:DFICT in their 2013 and 2015 consensus reports, as well as the EU,[362] Canada, the UK, New Zealand and others.[363] The main departures from this position are Russia and China, who are both actively distancing themselves from this assertion.[364]

a) UN Charter

The UN Charter[365] is a binding, foundational document to which all members of the United Nations must adhere. Considering first how it applies to the issue of outer space security and focusing extensively on the reference to the UN Charter in the Outer Space Treaty, experts of the 2019 GGE:PAROS[366] re-affirmed the relevance of the UN Charter principles in mitigating the risk to outer space assets, particularly as they relate to the prohibition of the threat or use of force,[367] the peaceful settlement of disputes,[368] the right of individual and

[360] Outer Space Treaty, *supra* note 8 at Art. 3.
[361] A Osula, H Roigas, *supra* note 270 at 7.
[362] European Union, Launching of the EU Cyber-Resilience for Development (Cyber4D) programme in Mauritius (Mauritius , 08 Feb 2019) online: <https://eeas.europa.eu/topics/health/57808/launching-eu-cyber-resilience-development-cyber4d-programme-mauritius_en>
[363] Joint statement made by the Permanent Representative of Canada to the UN on behalf of Australia, Chile, Estonia, Japan, the Netherlands, New Zealand, the Republic of Korea, the United Kingdom, and Canada on Information and Telecommunications in the Context of International Security (2018) online: <https://www.international.gc.ca/world-monde/international_relations-relations_internationales/un-onu/statements-declarations/2018-10-26-info_telecommunications.aspx?lang=eng>
[364] CCDCOE, *supra* note 164 at 5.
[365] Charter of the United Nations, Oct. 24, 1945, 1 U.N.T.S. XVI [UN Charter].
[366] UNODA, *supra* note 7
[367] UN Charter, Art. 2(4): "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the purposes of the United Nations"
[368] UN Charter, Art. 33: "The Parties to any dispute, the continuance is likely to endanger the maintenance of international peace and security, shall, first of all, seek a solution by negotiation, enquiry, mediation,

collective self-defence,[369] and the precedence of the UN Charter over other international obligations.

While, based on the above argument, there is little doubt that the UN Charter can play an important role in regulating the outer space environment, it is important to consider how this applies when combining this environment with that of cyber space.

Considering cyber-attacks specifically, Article 2(4) of the UN Charter asserts that all Members shall refrain from the threat or use of force against any State, or in any manner inconsistent with the purposes of the United Nations. When considering whether this applies, the first and most important consideration is whether a cyber-attack constitutes a 'use of force' for the purposes of the Charter. To help determine whether this is the case, it is instructive to review the International Court of Justice's *Legality of the Threat of Use of Nuclear Weapons* advisory opinion. In this case, the Court states that an attack can be considered a use of force "regardless of the weapons employed."[370] On the basis of this statement, a number of academics and policy-makers have asserted that a cyber operation of a certain gravity and consequence could constitute an armed attack, capable of triggering the right to self-defence – in such situations it is suggested that States are free to choose the appropriate means to respond, so long as that response is within the bounds of international law.[371] The Tallinn Manual supports this position, stating that cyber-attacks can amount to armed force if the consequences of the attack are comparable to those of a non-cyber-attack[372] (as determined by analysing the

concillation, arbitration, judicial settlement, resort to regional agencies or arrangements, or other peaceful means of their own choice."

[369] UN Charter, Art. 51: "Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security…"

[370] International Court of Justice, Legality of the Threat of Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, ¶39 (Jul. 8)

[371] CCDCOE, *supra* note 164 at 2.

[372] *Ibid* at 69.

scale and effects of such consequences).[373] Many (including this author) however, consider this to be an overreach in interpreting the UN charter.[374]

b) International Humanitarian Law

A significant point of discussion regarding the legality of carrying out a cyber-attack against outer space assets is whether such an attack falls outside of the fundamental principles of international humanitarian law (IHL) as codified under the 1977 Additional Protocol to the 1949 Geneva Conventions.[375] IHL, briefly, is a set of rules which seeks to limit the effects of an international armed conflict, protecting those not involved in hostilities, and restricting the means and methods of warfare used so as to ensure that excessive or indeterminate damage is not caused.[376] Before determining if cyber-attacks to outer space assets would run afoul of IHL, it is important to first examine if IHL applies to both outer space, and cyber space.

i. Applicability of IHL to Outer Space

It is perhaps important to note that the GGE:PAROS was apprehensive about even discussing the applicability of IHL to outer space, expressing concern that such discussions could signal acceptance of the notion that armed conflict could be conducted in outer space.[377] Should this concern be put aside, however, the general applicability of wider international law is clearly established in the Outer Space Treaty.[378] Given this, we would assert that there is no question that the overarching rules of IHL would apply to the outer space environment.

ii. Applicability of IHL to Cyber-attacks and Cyber Space

Under Article 36 of Additional Protocol I of the 1949 Geneva Convention, States are obligated to conduct a review prior to the development and deployment of new weapons to

[373] CCDCOE*, supra* note 164 *at 69.*
[374] A Osula, H Roigas, *supra* note 270 at 131.
[375] ICRC, A Guide to the Legal Review of New Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977 (International Committee of the Red Cross Geneva, January 2006) at 937
[376] ICRC, War and Law (accessed 5 December, 2019) online: <https://www.icrc.org/en/war-and-law>
[377] UNODA, *supra* note 7 at 7.
[378] Outer Space Treaty at Art. 3.

ensure that that weapon adheres to IHL.[379] An Article 36 review will cover "weapons, means or methods of warfare" and, according to the International Committee of the Red Cross' Commentary on the Additional Protocol, this would include weapons in the widest sense, in addition to the way in which such weapons are used.[380] This does make the material scope of Article 36 quite broad, covering weapons of all types (including anti-personnel or anti-material, lethal and non-lethal, and weapons systems in general) as well as the way weapons are used (such as in military doctrine, tactics and rules of engagement).[381] Given this, we would assert that cyber-attacks could be covered by IHL.

This approach is generally consistent in the international community, which is virtually united in stating that IHL should apply to cyber-attacks[382] with the UK, the US, [383] the EU,[384] France[385] and Russia,[386] all stating this to be the case. This was similarly expressed by the International Court of Justice, which stated that the principles and rules of IHL would apply to "all forms of warfare and to all kinds of weapons, those of the past, those of the present and those of the future."[387] The main source of potential opposition to this point of view would be China which, while not providing a definitive statement on IHL, considers that that there are no "general international rules in cyberspace that … govern the behavior" of states.[388]

---

[379] V Boulanin Implementing Article 36 Weapon Reviews in the Light of Increasing Autonomy in Weapon Systems (SIPRI Insights on Peace and Security, No. 2015/1, November 2015) at 2
[380] *Ibid*.
[381] ICRC, *supra* note *376* at 937.
[382] M Schmitt, *supra* note *31* at 3.
[383] Global Commission on the Stability of Cyber Space, *supra* note 29 at 9.
[384] *Ibid* at 32.
[385] France, "La Stratégie nationale pour la sécurité du numérique : une réponse aux nouveaux enjeux des usages numériques," Agence nationale de la sécurité des systèmes d'information" online: <https://www.ssi.gouv.fr/actualite/la-strategie-nationale-pour-la-securite-du-numerique-une-reponse-aux-nouveauxenjeux-des-usages-numeriques/>
[386] CCDCOE, *supra* note 91.
[387] International Court of Justice, Legality of the Threat of Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, ¶86 (Jul. 8)
[388] Group of Twenty "G20 Leaders Communiqué," online: <http://www.mofa.go.jp/files/000111117.pdf>; United Nations General Assembly, Report of the Group of Governmental Experts on Developments in the Field

iii. Outer Space, Cyber Space, and IHL

As mentioned, Article 36 of the Additional Protocol mandates that States who are in the process of studying, developing, acquiring, or adopting a new weapon or means of warfare must determine whether its employment would, in some or all circumstances, be prohibited by the principles of IHL or broader international law.[389]

In general, these principles of IHL include:[390]

i. The prohibition on indiscriminate targeting – Requires that a weapon be able to distinguish between military objectives and civilians (or civilian objects). In circumstances of doubt, that weapon should presume civilian status;[391]

ii. The rule of proportionality – Prohibits any "attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated;"[392]

iii. The rule of precaution – Mandates that all feasible precautions must be taken to avoid (or at least minimize) incidental harm to civilians and damage to civilian objects.[393]

In circumstances where a weapon is unable to comply with the above considerations, the State seeking to employ the weapon may need to attach conditions or comments to their approval, which will then be integrated into the rules of engagement or operating procedures associated with that weapon.[394]

---

of Information and Telecommunications in the Context of International Security, A/69/68 (June 24, 2013) online (pdf): <https://ccdcoe.org/sites/default/files/documents/UN-130624- GGEReport2013_0.pdf>

[389] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), Art. 36, 8 June 1977 [Geneva Convention Additional Protocol]

[390] Switzerland, Towards a "compliance-based" approach to LAWS (Informal Working paper submitted by Switzerland, 30 March, 2016) at [13]

[391] Geneva Convention Additional Protocol, Art. 48.

[392] *Ibid* at Art. 51

[393] *Ibid* at Art. 57

[394] ICRC, *supra* note 376 at 943

Applying the principles of discrimination, proportionality, and precaution to such a markedly new field such as cyber-attacks, specifically as they relate to outer space assets, is not a particularly easy task. The main concern in this circumstance is that such an attack is unable to be targeted in such a way that would definitively not cause excessive harm to civilians, thus potentially breaching all three of the aforementioned principles. As an example, certain satellites might be used both used for aerial imaging for military purposes and used also for disaster mitigation, and determining this to be the case before carrying out an attack could be nigh on impossible with current technology. As a result, this would mean that the destruction of a legitimate military target could potentially have a catastrophic effect on a large civilian population.[395]

Given the potential unknown flow-on effects that attacking an outer space asset may have (for example, in circumstances where an asset is used for both military and civilian purposes) combined with the lack of surety which applies when attacking an outer space asset (in regards to the assets purpose), this burden on States to ensure they do not breach these prohibitions is significant. As a result then, there may be a plausible case in saying that, any State who is in the process of designing/procuring/utilizing a cyber-weapon capable of causing destructive damage to an outer space asset, may well be violating international law if they have failed to consider IHL.

c) Summary

Of all international law, the most applicable provisions would be those contained in general law. However, while such general law contains firm, binding resolutions which hold States accountable for a wide range of actions – the applicability of such general international law to specialized environments such as outer space and cyber space, is difficult given the

[395] Otani, Oskami, Kahtake, "Dual-Use Concept on Civil and Defense Uses of Outer Space" at 2 (Japan Society for Aeronautical and Space Sciences and ISTS. January 2012)

unique nature of these environments. Given this lack of a determinative prohibition or control on the use of cyber-attacks on outer space assets (or indeed, the use of any attack to outer space assets), we would assert that a new instrument which clarifies this area of law is desperately needed. Part IV of this thesis will now consider the key principles which need be borne in mind in the construction of such an instrument.

PART IV

KEY PRINCIPLES TO BE BORNE IN MIND WHEN CONSIDERING NEW INTERNATIONAL INITIATIVES

While outer space has a greater number of multilateral treaties than one would expect for such a niche area, none of these treaties explicitly mentions that States are not permitted to attack another State's space assets.

Moreover, the legality of the operationalisation of cyber activities is still debated. Cyber activities have become a regular part of military operations, and legal issues surrounding conducting of cyber intelligence operations, the limits of State sovereignty, the threshold of armed attacks, and the right to self-defence are all issues which are, as of yet, unsettled.[396] States are expressing significant concern about the fact that such cyber threats are increasing in both number and impact, and that perpetrators are, in at least some circumstances, able to carry out destructive cyber actions with relative impunity.[397] Further, as mentioned, potentially over half of all States outside of Europe have admitted that they have insufficient frameworks for the criminalization and prosecution of extraterritorial cyber-crime acts.[398]

While States are currently divided on whether a new treaty instrument is required to manage the threat that cyber-attacks pose to outer space assets,[399] it is the position of the present

[396] CCDCOE, *supra* note 164 at 3.
[397] HM Government, *supra* note *77* at 18.
[398] UNODC Study on Cybercrime, *supra* note 24 at xxiv.
[399] CCDCOE, *supra* note 164 at 5.

author that the current international regime is inadequate with regard to security in both outer space and cyber space and that new instruments are indeed required. The key principles which need be borne in mind when considering how to fashion these new instruments, including the form they should take and the areas which they should cover, will be discussed in this Part.

A. What form should a new instrument take?

Before considering individual provisions, it is important to first determine the form that any new instrument should take, including the parties it should include, the degree to which its provisions are mandatory, and the ability of the instrument to adapt through time.

1. Membership

The first step in considering any international agreement is to determine the desired circle of parties to that agreement, namely, whether it should be a multilateral, plurilateral (or regional), or bilateral agreement.

Multilateral treaties are especially useful for the purpose of widely enforcing harmonization in an area of policy conflict, preventing fragmentation at the international level that could produce undesirable diversity of laws, jurisdictional bases, and mechanisms of cooperation.[400] Given the goal of ensuring maximum compliance in the complex interface between cyber space and outer space, and also given that current instruments and regions reflect significant divergences (particularly relating to cyber law), it can certainly be argued that a multilateral treaty would be desirable.[401] To discuss this possibility, however, it is helpful to consider those who are supporting and those who are opposing reaching consensus on such an agreement.

To begin with, China has supported a multilateral approach to governing cyberspace, suggesting that the United Nations should take a leading role in building international

[400] UNODC Study on Cybercrime, *supra* note 24 at xxiv.
[401] *Ibid*.

consensus on rules to regulate online activity.[402] Given that China has also advocated strongly for a binding outer space security treaty (particularly in the Russia/China Draft Treaty on Placement of Weapons in Outer Space)[403] it would seem fairly likely to support a multilateral treaty. India, too, has argued in favour of creating new bodies within multilateral institutions such as those hosted by the UN and modelled on the Committee for the Peaceful Uses of Outer Space.[404]

In this narrow group of superpowers, the United States have been the least enthusiastic about joining a multilateral security Agreement, often citing a lack of comprehensiveness or common definitions as reasons for not supporting such instruments.[405] The United States has done this with respect to both outer space instruments[406] and cyber treaties[407] (with the exception of the Budapest Convention).

The importance of having these key 'superpower' States (such as China, the US, Russia, and India) on board to any agreement cannot be overstated. While, of course, multilateral security agreements require consensus of all ratifying parties, political realism dictates that these superpowers are both more guarded in their security concerns, and have more political sway to bring their regional allies across the line.[408] As such, bridging the misunderstanding

---

[402] Global Commission on the Stability of Cyber Space, *supra* note 29 at 13.
[403] Reaching Critical will, Conference on Disarmament GE 02-42978 (CD/1679) (2002) <http://www.reachingcriticalwill.org/images/documents/Resources/Factsheets/paros/CD1679.pdf>
[404] Council on Foreign Relations, "The UN GGE on Cybersecurity: What is the UN's role?" (April 15, 2015) online: <https://www.cfr.org/blog/un-gge-cybersecurity-what-uns-role>; as per Global Commission on the Stability of Cyber Space, *supra* note 29 at 9.
[405] Considering what has often been interpreted as a lack of engagement from the US-side to resolve these alleged mis-steps in Agreement drafting, conjecture would suggest that this unwillingness to participate in such a multilateral is the result of a lack of trust between States, as opposed to a genuine disagreement on how an Agreement should be structured.
[406] Conference on Disarmament "Analysis of the 2014 Russian-Chinese draft "treaty on the prevention of the placement of weapons in outer space, the threat or use of force against outer space objects" (PPWT) (CD/1985)" CD/1998 (2014) <https://documents-dds ny.un.org/doc/UNDOC/GEN/G15/007/57/PDF/G1500757.pdf?OpenElement>
[407] Global Commission on the Stability of Cyber Space, *supra* note 29 at 16.
[408] J Jakóbowski "Chinese-led Regional Multilateralism in Central and Eastern Europe, Africa and Latin America: 16 + 1, FOCAC, and CCF" at 668 (2018) Journal of Contemporary China, Volume 27, Issue 113, 2018, 659-673

(or mistrust) between these superpowers would be crucial to reaching agreement between a large number of States in a mega-multilateral.

If we were to analyse trends of convergence of opinion from these States (and, indeed, all States) on multilateral agreements, it may be simply unrealistic to expect a multilateral agreement of any significance.[409] Multilateral Agreements on security issues are increasingly rare, as demonstrated by the fact that the Conference on Disarmament (the United Nations primary Treaty making body on disarmament issues) has been unable to come to consensus on any issue since 1996,[410] as well as by the fact that every successive agreement following the Outer Space Treaty has had fewer ratifying parties than the last. Given this, while a mega-multilateral may be desirable for purposes of consistency amongst a large number of States, such consistency may, instead, need to be built through a larger number of treaties with fewer parties.

The establishment of further regional agreements are an appropriate middle ground in this regard. While they do suffer the limitations of fewer parties than multilateral treaties, they do bring together a number of States with similar viewpoints on a number of key issues and, as demonstrated at [*Part III(B)*], can prove extremely effective in terms of developing norms and providing crucial research and technical and policy development.

Bilateral agreements, too, have shown themselves to be an effective tool for the provision of formal mutual legal assistance and security measures.[411] As discussed at [*Part III(A)*], a number of such bilateral agreements had a significantly positive impact in lowering cyber-attacks against both government and industry.[412] Bilateral agreements can be a positive

[409] The key to resolving this issue may likely be in building the trust between these key superpowers to increase likelihood of reaching agreement. Resolving this geopolitical issue, however, is unfortunately beyond the scope of this thesis.
[410] Nuclear Threat Initiative "Conference on Disarmament" (April 27, 2017) online: <http://www.nti.org/learn/treaties-and-regimes/conference-on-disarmament/>
[411] UNODC Study on Cybercrime, *supra* note 24 at xxv.
[412] Adam Segal, *supra* note 239; as per Global Commission on the Stability of Cyber Space, *supra* note 29 at 25.

way to begin building agreement between States, particularly as they can strive for something significantly more ambitious than multilateral treaties given the narrow number of parties. The limitations of bilateral agreements however, are clearly that they do very little in terms of harmonizing policy on a global scale.

2. Binding or non-binding

A fundamental consideration for any new agreement is whether to pursue binding or non-binding provisions. While some cyber-crime agreements, such as the Shanghai Cooperation Organization Agreement[413] and the Budapest Convention on Cyber-crime,[414] have managed to secure binding provisions, such binding provisions are remarkably difficult to negotiate, and can be too inflexible to respond to an ever-changing threat such as cyber-attacks.[415]

Inspiration could perhaps be drawn, *mutatis mutandis,* from aviation cyber policy which utilizes non-binding initiatives extensively. Even in 'hard law' instruments such as the Chicago Convention,[416] the language in the cyber focused Annex 17 utilizes non-binding language, recommending that "each Contracting State should develop measures in order to protect information and communication technology systems used for civil aviation purposes from interference that may jeopardize the safety of civil aviation."[417]

It is also important to note that, even if States manage to secure a full binding agreement, establishing non-binding norms between States can always be seen as a valuable exercise (and can be included as part of that agreement), and should be pursued as a priority[418]

---

[413] SCO, *supra* note *282*
[414] Budapest Convention, *supra* note 12.
[415] UNODC Study on Cybercrime, *supra* note 24 at xxiv.
[416] Convention on International Civil Aviation, 7 December 1944, 15 UNTS 295 (entered into force on 4 April 1947) [Chicago Convention]
[417] ICAO, Annex 17 to the Convention on International Civil Aviation: Security: Safeguarding International Aviation Against Acts of Unlawful Interference (ICAO, 10th Edition, April 2017) at 4.9, online (pdf): <http://dgca.gov.in/intradgca/intra/icao%20annexes/an17_cons.pdf>
[418] Global Commission on the Stability of Cyber Space, *supra* note 29 at 30.

in order to help set State expectations about behaviour.[419] Helpfully, the Microsoft corporation proposed a series of norms for States, recommending that they should exercise restraint in developing cyber weapons and ensure that any which they do develop are limited, precise, and not reusable, and also that States should not proliferate cyber weapons.[420]

The optimum outcome could perhaps then be to develop hard, binding provisions for those core principles of an Agreement (such as mandating that deliberate attacks not be carried out on outer space assets), and non-binding provisions for those principles which require greater adaptability, such as cyber security industry standards which ensure constant innovation, capacity build-up, and maintenance.

Such non-binding provisions could also be more flexible in their implementation than those binding provisions, potentially being developed and agreed upon by an international community made up of cyber capable States and other critical stakeholders within the international space/cyber supply chain and insurance industry, who work collectively to develop a space cyber security regime which is competent to match the range of threats currently facing the industry.[421]

B. What provisions should be included in negotiated instruments?

Having considered the general form that the instrument could/should take, it is now important to consider the individual provisions which should be considered in any new instrument. In this section, it is important to note that, while this thesis focuses specifically on how cyber-attacks can impact outer space assets, the narrow scope of this focus may unnecessarily restrict the possibility of States reaching consensus on this issue. As such, many of those thematic areas for policy development outlined below have been advanced in

[419] A Osula, H Roigas, *supra* note 270 at 133.
[420] Microsoft, "From Articulation to Implementation: Enabling progress on cybersecurity norms," online (pdf): <https://mscorpmedia.azureedge.net/mscorpmedia/2016/06/Microsoft-Cybersecurity-Norms_vFinal.pdf>; as per Global Commission on the Stability of Cyber Space, *supra* note 29 at 28.
[421] D Livingston, P Lewis, *supra* note 19 at v.

line with a broader objective of governing cyber-activities and protecting pieces of national infrastructure.

1. Consensus on Criminal acts

Perhaps the most important point of discussion in any international security treaty is to develop consensus on what constitutes a criminal act, as this will permeate in to every other facet of the agreement. Ensuring harmonization of laws between States is essential for, *inter alia,* the elimination of criminal safe havens and global evidence collection.[422]

Divergences in national cyber-crime laws derive from a range of factors, including underlying legal and constitutional differences.[423] This pattern of divergence needs to be taken into account when approaching any negotiation. The development of model legislation (such as the COMESA draft model bill) is helpful, though if States have no will to adopt such measures, then their efficacy is limited.

In this regard, mandating the implementation of certain rules into ratifying parties' domestic legislation, such as that outlined at [*Part II(B)(2)*] of this thesis, as well as those more general areas of domestic law outlined in the 2012 ITU/CARICOM/CTU policy guidelines,[424] would be a valuable first step.

2. Jurisdiction

Determining which State has jurisdiction in the case of an attack is a fundamental part of any international security treaty. While we have seen individual States attempting to address this issue (i.e. by expanding extraterritorial jurisdiction over data)[425] at this point there is still

[422] UNODC Study on Cybercrime, *supra* note 24 at 56.
[423] *Ibid.*
[424] International Telecommunication Union, *supra* note *144*.
[425] For example, see the US CLOUD Act (part of the Consolidated Appropriations Act, 2018, H.R. 1625).

no international consensus on how jurisdiction in circumstances of transnational cyber-attacks is best handled.

The natural starting point for jurisdiction (without a negotiated agreement) will always emerge from one point: sovereignty. Law enforcement and criminal justice matters will always fall within the exclusive domain of the sovereign State, which has traditionally been linked with geographical territory. This means that, without a treaty or other consent, a person who attacks hypothetical State A from their hometown of hypothetical State B, is unable to be arrested by State A, may not be served a summons by State A, and may not be subject to police or tax investigations mounted against them by State A.[426] This would also be the case even if the perpetrator was a citizen of State A who was taking shelter in State B.[427]

International law has provided a number of ways in which jurisdiction over cyber-crime can be addressed. The most effective of jurisdiction provisions would appear to be nationality-based jurisdiction,[428] which requires a State to ensure jurisdiction when the act has been committed by one of its nationals (including outside of the national territory).[429] Another common jurisdiction provision is territory-based jurisdiction, which requires a State to exercise jurisdiction over any offence which is committed within the State's geographical territory.[430] Given the complex nature of cyber-crime, some States have amended their jurisdiction provisions to ensure that territorial jurisdiction can be asserted even in circumstances where the "whole" offence has not taken place in a State, instead allowing elements or effects of the act (or the location of the computer systems or data utilised) to develop territorial linkages.[431]

---

[426] UNODC Study on Cybercrime, *supra* note 24 at 182.
[427] Cassese, "International Law" (2nd ed. Oxford: Oxford University Press, 2005) at 53.
[428] There is also so-called called 'passive nationality' requires States to establish jurisdiction over an offence committed outside of the territory against 'one of its nationals,' though, while these are often used in cases which concern the rights of children, it will not necessarily be applicable to the present circumstances. For example, see: EU Directive on Child Exploitation (2011/93/EU), Art. 17(2)(a).
[429] See COMESA Draft Model Bill, Art.40(c); Commonwealth Model Law, Art. 4(d); Budapest Convention, Art. 22(1)(d); and League of Arab States Model Law 2004, Art. 30(1)(d).
[430] UNODC Study on Cybercrime, *supra* note 24 at 189.
[431] *Ibid*.

When introducing jurisdiction into an international agreement, it is also worth considering the following principles which can be incorporated into such provisions:

iv. The protective principle – extends competence over offences affecting "an overriding interest of the State";[432]

v. Extradite or prosecute – In cases where hypothetical State B has apprehended an offender who is eligible to be extradited to State A under an international agreement, State B can decide whether to either extradite that offender, or prosecute them under their domestic legislation. Generally, in agreements where an 'extradite or prosecute' provision is included, there will be a requirement for uniform criminalization (and minimum penalties) of offenses between those State parties;[433]

vi. Prioritization of jurisdictions – In cases where more than one State has a basis on which to assert jurisdiction over an act (so-called 'concurrent jurisdiction'), it is important that these claims are prioritised. The League of Arab States Convention has addressed this issue, providing a detailed order of priority for competing jurisdictional claims in the following order: (i) States whose security or interests have been disrupted by the offence; (ii) States in whose territory the offence was committed; and (iii) the State of nationality of the offender. In circumstances where a balance cannot be found in that order, then priority is afforded to the first requesting State.[434]

The issue of jurisdiction is perhaps one of the most vital in any treaty, as it allows overseas law enforcement agencies to work together to ensure that fewer places exist where

[432] For example, please see the League of Arab States Convention, Art. 30(1)(e).
[433] For example, please see the COMESA Draft Model Bill, 2011, Art. 40(d); Budapest Convention, Art. 22(3); League of Arab States Convention, Art. 30(2); ITU, *supra* note 143 at Art.4(3).
[434] UNODC Study on Cybercrime, *supra* note 24 at 195.

cyber criminals feel free from investigation and prosecution, thereby increasing their ability to disrupt and prosecute cyber criminals in hard-to-reach jurisdictions.[435]

3. Extradition

When jurisdiction has been established between two States and a perpetrator needs to be extradited between those States, it is important that rules are in place to govern this exercise.[436]

In this regard, it is helpful to factor expediency in to any potential Agreement. A recent UNODC study found that, in circumstances where States requested extradition through formal mechanisms, response times were reported to be in the order of months.[437] This long timescale has reportedly presented challenges in the collection of electronic evidence. To combat this, some States[438] have channels established for urgent requests, though how effective these have been is unclear.

To further assist the early capture of evidence, it has been suggested that initiatives for informal cooperation and for facilitating formal cooperation, such as using 24/7 networks (as included in a range of US bilaterals and discussed at [*Part III(A)*]), can be effective, although informal contact points between States are reportedly utilised only on rare occasions (approximately 3% of all reported cyber-crime cases).[439]

4. Private Sector Interaction Management

As mentioned specifically in the 2011 SCO "Agreement on Cooperation in the Field of Information Security"[440] at [*Part III(B)(2)*] and at numerous other times in this thesis, it

[435] HM Government, *supra* note *77* at 63.
[436] Such principles have been discussed in two binding instruments (the Budapest Convention and the League of Arab States Convention), and one non-binding instrument (the COMESA Draft Model Bill) make specific mention of extradition in relation to cyber-crime. As per UNODC Study on Cybercrime, *supra* note 24 at 199-200.
[437] UNODC Study on Cybercrime, *supra* note 24 at xxv.
[438] Sixty per cent of countries in Africa, the Americas and Europe, and 20 per cent in Asia and Oceania, as per UNODC Study on Cybercrime, *supra* note 24 at xxv.
[439] *Ibid.*
[440] Shanghai Cooperation Organization, *supra* note 282.

has become a relatively common provision among international cyber agreements to mandate that States do not allow (or require) their private sector ICT companies to insert vulnerabilities into their products.

The need for States to mitigate the threat of backdoors being surreptitiously introduced in hardware or software is of significant concern[441] (a concern which is shared by private sector[442] and gaining significant publicity what with the recent security controversy surrounding the Huawei mobile phone providers),[443] and should continue to be addressed in any new cyber-focused Agreement.

5. Transparency and confidence building

Given that both cyber and outer-space security are attracting significant interest from States, the risk of conflict resulting from mistrust, misunderstandings and miscalculation is growing significantly.[444] As discussed at numerous points throughout this thesis, one of the fundamental tools for helping States to avoid escalation and miscalculation is that of Transparency and Confidence Building Measures (TCBMs).

Many existing TCBMs date back to 1975 when the Helsinki Final Act[445] was adopted, which helped to prevent a potential outbreak of military conflict by improving relations between government officials and militaries.[446] Since that time, these measures have been fundamental in resolving a number of issues, proving to be a significant stabilizing factor in conflicts the world over.[447]

---

[441] Global Commission on the Stability of Cyber Space, *supra* note 29 at 30.
[442] Microsoft, *supra* note *419*; as per Global Commission on the Stability of Cyber Space, *supra* note 29 at 28.
[443] S Lohr, "U.S. Moves to Ban Huawei From Government Contracts" (NY Times, 7 August. 2019) online: <https://www.nytimes.com/2019/08/07/business/huawei-us-ban.html>
[444] A Osula, H Roigas, *supra* note 270 at 130.
[445] OSCE, 'Conference on Security Co-operation in Europe: Final Act' (Organization for Security and Co-operation in Europe, Conference on Security Co-operation, Helsinki, 1975) online: <https://www.osce.org/mc/39501?download=true>
[446] *Ibid*.; as per A Osula, H Roigas, *supra* note 270 at 132.
[447] Such as in the 1972 US/USSR bilateral SALT agreement

In the context of the Prevention of an Arms Race in Outer Space (PAROS), the use of TCBMs to help manage risks of miscalculation and mistrust has reached consensus (though many States, and the GGE:PAROS itself, [448] have emphasised the fact that voluntary TCBMs could not substitute for legally-binding measures).[449]

The development of TCBMs to reduce risks in cyberspace has also been supported by most key cyber States, including explicitly by the US, France,[450] Russia,[451] the UK,[452] and the EU[453] in their State policy documents.[454] Given this wide acceptance from a wide number of key 'power' States, cyber focused TCBMs can play a key role reaching cyber stability through enhancing States' understanding of their rival's actions online.[455]

Building on some of those TCBMs discussed in earlier portions of this thesis (particularly in those bilateral agreements discussed at [*Part III(A)*] and as suggested by the GGE:DFICT) a new instrument could also potentially include:[456]

i. Communication and information exchange measures which enhance mutual understanding of national military capabilities and activities through facilitating regular communication. This can be done by ensuring military points of contact, including hotlines between chiefs of armed forces, an exchange of military information on national forces and armaments, and advanced notification of important military exercises;

[448] UNODA, *supra* note 7 at 12.
[449] UNODA "Report of the Secretary-General on transparency and confidence-building measures in outer space activities" (2017) <https://www.un.org/disarmament/topics/outerspace/sg-report-outer-space/>
[450] Global Commission on the Stability of Cyber Space, *supra* note 29 at 36-37.
[451] CCDCOE, *supra* note 91.
[452] Global Commission on the Stability of Cyber Space, *supra* note 29 at 13; see also HM Government, *supra* note *77* at 63.
[453]European Commission "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace," online (pdf): <http://eeas.europa.eu/archives/docs/policies/eu-cyber security/cybsec_comm_en.pdf>
[454] Global Commission on the Stability of Cyber Space, *supra* note 29 at 14.
[455] *Ibid* at 9.
[456] A Osula, H Roigas, *supra* note 270 at 134.

ii. Social and cultural measures, whereby ties are strengthened between communities through people-to-people dialogues and joint projects. These discussions could be focussed around protection of space assets/national infrastructure, domestic cyber strategies, and the scope, administrative structures and institutional settings which help to assist in the areas of cyber defence;[457]

iii. Focusing more widely on 'responsibility rules for States', fostering data-exchange, bilateral/regional consultations, the exchanging of white papers, the establishment of point-of-contact networks and hotlines (including procedures and templates on their use), the fostering of CERT-to-CERT collaboration, and encouraging law enforcement collaboration;[458]

iv. Microsoft has also recommended that States have a clear policy on the handling of vulnerabilities which favours responsible disclosure instead of stockpiling or selling those vulnerabilities on to other State or private actors.[459] Similar measures were also supported by the GGE:DFICT and the OSCE.[460]

6. Gathering crime statistics data

By understanding the extent of harms, losses and illicit financial gains caused by cyber-crime, States are better able to prioritize their interventions. In line with this, encouraging States to gather crime statistics is a fundamental (albeit difficult) task.[461] While there is some degree of cross-national comparability for these means, to make this sharing truly useful, there needs to be a consensus on what constitutes cyber-crime (as discussed at

[457] J Lewis, G Neuneck, *supra* note 23 at 137.
[458] Global Commission on the Stability of Cyber Space, *supra* note 29 at 30; Institute for Peace Research and Security Policy at the University of Hamburg, Challenges in Cybersecurity: Risks, Strategies, and Confidence Building, Institute for Peace Research and Security Policy at 14 (University of Hamburg, 2011) online (pdf): <https://www.unidir.org/files/medias/pdfs/conference-report-eng-0-373.pdf >
[459] Microsoft, *supra* note 419; as per Global Commission on the Stability of Cyber Space, *supra* note 29 at 28.
[460] Global Commission on the Stability of Cyber Space, *supra* note 29 at 28.
[461] UNODC Study on Cybercrime, *supra* note 24 at 24.

[*Part IV(B)(3)*]). What is also clear is that any statistics which measure "cyber-crime" as a single phenomenon are unlikely to be comparable cross-nationally, due to significant variations in the content of the term between recording systems.[462]

While the best approach to gather such data is as of yet unsettled, one method which has gained support is to provide data disaggregated by different cyber-crime acts, potentially sourced from four primary information points including: police-recorded crime statistics, population-based and business surveys, victim reporting initiatives, and technology-based cybersecurity information.[463] In amongst those data sources, it is useful to gather a range of information, such as details of the perpetrators, details on flows within illicit markets, and information on numbers of criminal events, harms and losses.[464]

7. Sharing threat data

As discussed at [*Part II(B)(6)*], it is important that States share data of threats they encounter. This ensures that those have an accurate assessment of the risk which cyber-attacks pose, and a sense of what the latest threats might be.

To combat the under-sharing of cyber-attacks, States could potentially establish, as a part of any new agreement, a network where threat information can be anonymously shared (such as by revealing "'indicators of compromise")[465] so as to better enable governments and private entities to understand the landscape of threats they face.[466]

---

[462] UNODC Study on Cybercrime, *supra* note 24 at 24.
[463] *Ibid* at 25.
[464] *Ibid.*
[465] Defined as pieces of "forensic data, such as data found in system log entries or files, that identify potentially malicious activity on a system or network"; as per N Lord, What are Indicators of Compromise (Digital Guardian, September 11, 2018) online: <https://digitalguardian.com/blog/what-are-indicators-compromise#:~:targetText=Indicators%20of%20compromise%20(IOCs)%20are,on%20a%20system%20or%20network.%E2%80%9D>
[466] C Baylon, *supra* note *22* at 13.

8. Gathering and disclosing vulnerability data

The collection of vulnerability data is important to prevent and reduce crime, to enhance local, national, and international responses and to identify gaps in responses.[467] By gathering this data, States are also in a better position to provide intelligence and risk assessments and to educate the public through the disclosing of those vulnerabilities, either in a public or localized manner.[468]

The 2015 GGE:DFICT Consensus Report, the OSCE, and the private sector have all recommended that States develop vulnerability disclosure policies which demonstrate how State security agencies discover computer vulnerabilities and inform vendors.[469]

9. Focus on outer space assets or critical infrastructures (including space assets)

Manifestly, if outer space assets are to be protected from cyber-attacks by a proposed agreement, then those assets will need to be explicitly included in that agreement. However, should an agreement which focuses specifically on the risk of cyber-attacks on outer space assets be too specific to gain consensus, then a compromise could be to open this agreement to include all critical infrastructures.

A useful reference point for the latter is provided in the legally binding European Council Directive on the identification and designation of European critical infrastructures[470] discussed at [*Part III(B)(1)(b)*], which includes cyber infrastructure specifically within its definitions. However, if this Directive were to be built upon for current purposes, outer space assets would need to be more explicitly mentioned (as opposed to just alluded to).

[467] UNODC, Guidelines for the Prevention of Crime, annex to United Nations Economic and Social Council Resolution 2002/13 on Action to promote effective crime prevention (24 July 2002) online: <https://www.unodc.org/documents/justice-and-prison-reform/crimeprevention/resolution_2002-13.pdf>
[468] *Ibid.*
[469] Global Commission on the Stability of Cyber Space, *supra* note 29 at 30.
[470] 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

10. Providing assistance

While States and industry alike no doubt would all like to protect their assets, many require technical assistance to carry out prevention, investigation, and prosecution of cyber-crime.

Regional organizations, such as the African Union, the OAS, and the Council of Europe, are recognised as providers of technical assistance by 20 per cent of responding countries in UNODC studies.[471] On a similar note, a range of both binding[472] and non-binding[473] regional instruments outlined at [*Part III(B)*] specifically provide for legal assistance.[474]

In relation to the specific assistance required, "general cyber-crime investigations" is reportedly the area where technical assistance is required most frequently, and also the area where most States reported receiving assistance.[475] While technical assistance can be short term, medium term and long term, most assistance lasts for less than one month, with only approximately 25% lasting for over two years.[476]

In this context, it is important in any agreement to include provisions where assistance can be refused. As an example, such provisions are included amongst those regional agreements discussed earlier, providing circumstances wherein legal assistance can be refused, such as when execution is contrary to national legislation, when the request concerns a political offence, or when the request is likely to prejudice sovereignty, security, public order, or other essential interests.[477]

---

[471] Australia, *supra* note *147* at 21.
[472] Please see the Commonwealth of Independent States Agreement, the Budapest Convention, and the League of Arab States Convention
[473] Please see the COMESA Draft Model Bill
[474] UNODC Study on Cybercrime, *supra* note 24 at 199-200.
[475] *Ibid* at 179.
[476] Australia, *supra* note *147* at 21.
[477] UNODC Study on Cybercrime, *supra* note 24 at 199-200.

11. Capacity building

Whereas the notion of "providing assistance" involves States lending resources or knowledge to other States for a specific task, capacity building involves teaching those States to assist themselves in the future. Not all States have the resources, skills, or expert knowledge to develop domestic cyber defence institutions, and capacity building in the form of joint workshops and exercises can help tremendously to increase security and build confidence.[478] Additionally, such efforts bring State's internal law into line with global practices,[479] allowing these States to abide by norms and participate in TCBMs.[480]

In a UNODC study, 75% of responding States across all regions reported requiring technical assistance in some thematic area linked with cyber-crime, while 70% of States reported providing some form of technical assistance to other States.[481] The United Kingdom has encouraged capacity building regularly, stressing its importance at the 2011 London Conference on Cyberspace, and subsequent conferences in Hungary (2012), Seoul (2013), the Netherlands (2015), and India (2017).[482] France has also placed significant emphasis on capacity building in order to reduce the threat that cyber-attacks pose to critical infrastructure.[483]

There are numerous areas in which capacity-building can be particularly useful – including helping States to establish and build the capabilities of national CERTs, assisting

[478] J Lewis, G Neuneck, *supra* note 23 at 137.
[479] Australia, *supra* note *147* at 32.
[480] Global Commission on the Stability of Cyber Space, *supra* note 29 at 9.
[481] UNODC Study on Cybercrime, *supra* note 24 at 178.
[482] United Kingdom, "London Conference on Cyberspace: Chair's statement" (2 November 2011) online: <https://www.gov.uk/government/news/london-conference-on-cyberspace-chairs-statement>; United Kingdom, "UK Non Paper On Capacity Building-Budapest Conference" (Budapest Conference on Cybersecurity 2012, 4-5 October, 2012) online: <https://web.archive.org/web/20130530035614/http:/www.cyberbudapest2012.hu/index>; United Kingdom, "Seoul Framework for and Commitment to Open and Secure Cyberspace," (Seoul Conference on Cyberspace, 2013); "Global Conference on Cyberspace 2015," United Kingdom, GCCS (2015) online: <https://www.gccs2015.com/>; United Kingdom, "5th Global Conference on Cyberspace," (GCCS, 2017) online: <https://gccs2017.in/>;as per Global Commission on the Stability of Cyber Space, *supra* note 29 at 13.
[483] France, *supra* note *385*.

developing countries to keep abreast of international policy developments,[484] developing State's capacity to enhance international cooperation, prosecution, trial support and digital forensics, or supporting States to endorse and operationalize the GGE recommendations.[485]

Similar to those assistance providing provisions outlined in the previous section, capacity building can be built into any new agreement. Such provisions will most often take the form of non-binding encouragements to provide assistance, or through the development of a body which helps to facilitate capacity building in key areas of interest in the Agreement.

12. Obtaining stored data

As mentioned at [*Part II(B)(3)*], the issue of obtaining stored data is a particularly significant one, especially given the challenges arising from the fact that data tends to be held by private entities. The inclusion of provisions which ensure investigative powers to allow the obtaining of data, both stored and in real time, is an important consideration in any international instrument. Such provisions can be found in five of the regional cyber-crime instruments discussed earlier[486] and have proved to be very effective. Orders for data are also an important investigative measure for obtaining stored computer data and, in this regard the Mauritius 'preservation order',[487] discussed at [*Part II(B)(3)(a)*] is a particularly important measure to build upon for inclusion in an international Agreement.

It is important to note, however, that the existence of such powers to obtain stored data does not, in itself, oblige service providers to collect or retain information they would not otherwise, meaning that States need to consider if they also need to mandate providers to store and retain relevant data for a certain period of time. This has been considered in

[484] Such as GA57/239 - Global Culture of Cybersecurity (as discussed at [Part III(C)(2)(c)]),
[485] Global Commission on the Stability of Cyber Space, *supra* note 29 at 38.
[486] COMESA Draft Model Bill, Art. 36(a); Commonwealth Model Law, Art.15; Budapest Convention, *supra* note *12*. At Art. 18(1)(a); ITU/CARICOM/CTU Model Legislative Texts, Art.22(a); League of Arab States Convention, Art. 25(1).
[487] Mauritius, *supra* note *182* at Part III, s11 <http://www.ncb.mu/English/Documents/Legislations/Computer%20Misuse%20and%20Cyber-crime%20Act%202003/misuse.pdf>

numerous international cyber-crime instruments, which contain provisions preventing the deletion of computer data important to cyber-crime investigations, with some instruments requiring individuals in control of computer data to preserve and maintain the integrity of the data for a specified period of time.[488]

13. Encouraging best practices

As discussed extensively at [*Part I(1)(b)*] and [*Part II*], the establishment of best practice guidelines to inform States how they can best protect their assets is crucial. The UK has stated as much in their National cyber security strategy, promoting the idea of making cyberspace "more secure by design" and promoting best practice.[489] The development of such best practice guidelines can be accomplished as part of an international agreement, as demonstrated in the aviation regulating Chicago Convention, which introduced SARPs as a non-binding collation of best practices.[490]

One limiting issue with regard to best practices that one must bear in mind though is that such practices often tend to be adhered to, up until the point where there is a significant financial implication required to adhere to it (as indicated by the fact that the Chicago Convention aviation SARPs have approximately a 33% rate of full State compliance).[491] While not much can be done about this in the short term, it does imply that best practices, while helpful, alone will not suffice to mitigate a threat.

14. Interaction with private sector

As mentioned at [*Part II(B)(5)*], given the fact that most attacks are carried out against private sector, their skill, knowledge, and experience in dealing with cyber threats is of crucial importance. The Microsoft Corporation has proposed a series of norms for States, recommending that States should assist the private sector to detect, contain, respond to, and

[488] UNODC Study on Cybercrime, *supra* note 24 at 126.
[489] HM Government, *supra* note *77* at 63.
[490] Chicago Convention, art. 37.
[491] ICAO, *supra* note 416 at 4.9.

recover from events in cyberspace.[492] Ensuring a general culture of cybersecurity by encouraging domestic stakeholders to be aware of cybersecurity risks (and providing them the steps to mitigate those risks) was also a key focus of UNGA resolution 57/239[493] discussed at [*Part III(C)(2)(c)*].

Another approach would be to recruit particular private operators to maintain a watching brief over any meetings arising from any concluded agreement, essentially acting in the same "whistleblower" capacity as any State signatory.[494] This innovation would offer a unique perspective, and could also allow State organizations to demand a particular standard of care in securing the network's core services and infrastructures.[495]

15. A normative approach

Particularly if it is found that coming to a full and comprehensive multilateral agreement is not possible, an alternative could be to take a 'normative approach'. This could take the form of a restriction on the first use of cyber weapons against outer space assets.

While such "no first use" statements have been criticised as easily reversible and, of course, unable to guarantee that potential aggressors are not preparing themselves for such an attack (in preparation of being the 'second' or 'third' to use such a weapon), a number of States have been strong proponents of such normativity, at least as an interim measure.[496]

Normative statements like these have been used in a variety of domains. Perhaps the most notable is the annually adopted "no first placement of weapons in outer space" precept, most recently introduced to the UNGA by Russia and China, encouraging all States to consider

[492] Microsoft, *supra* note *419*; as per Global Commission on the Stability of Cyber Space, *supra* note 29 at 28.
[493] United Nations General Assembly, Creation of a Global Culture of CyberSecurity, GA57/239 LVII A/RES/57/239 (2003) online (pdf): <https://www.oecd.org/sti/ieconomy/UN-security-resolution.pdf>
[494] R. Weber, R. Gunnarson, "A Constitutional Solution for Internet Governance" (18 Columbia Science and Technology Law Review, 2012) at 71; as per Global Commission on the Stability of Cyber Space, *supra* note 29 at 90.
[495] *Ibid*.
[496] J Lewis, G Neuneck, *supra* note 23 at 136.

upholding a political commitment not to be the first to place weapons in outer space.[497] This initiative has most recently been approved in December 2016[498] with a vote of 130 in favour (including members of the G-21[499] and Brazil)[500] to four against (Georgia, Israel, Ukraine, and the United States), with 48 abstentions (including Australia, Canada, New Zealand, the United Kingdom, Sweden, and Switzerland). Russia has stated that it supports the implementation of this initiative on a national, bilateral. and multilateral level, and believes this undertaking to be a flexible political commitment which will help to diminish the potential of an arms race being carried out in space.

The US has been a pronounced critic of Russia and China's no-first-placement initiative, considering it to be 'ambiguous' (in that it implicitly allows States to be the second or third to place weapons in outer space), lacks definitions (specifically for space weapons), lacks verification mechanisms, and does not address terrestrial-based ASATs (including cyber weapons).[501]

16. Facilitation of civil action across borders

As mentioned at [*Part II(A)(6)*], the use of civil legal action to both discourage cyberattacks and remedy the consequences of such acts is an emerging and important practice being pursued by the private sector. While, generally, international security issues are addressed through the international harmonization of national criminal laws so as to foster cross-border enforcement and prosecution of offenders (as provided for in the majority of those proposed thematic areas for policy action previously outlined in this section), given the

[497] UNIDIR, An update on "Outer Space Security" and a brief history of the prevention of an arms race in outer space, at 12 (presentations to inform CD Subsidiary Body 3 discussion, 23 May 2018) online (PDF): <https://www.unidir.org/files/medias/pdfs/presentation-to-inform-cd-subsidiary-body-3-discussion-eng-0-778.pdf>
[498] UNGA, No first placement of weapons in outer space, A/RES/71/32 (5 December, 2016)
[499] Indonesia on behalf of member States of G-21 "Working paper: Prevention of an arms race in outer space (PAROS)" CD/2031 (2015) At 3
[500] UNODA, *supra* note *447*.
[501] H Liu, F Tronchetti United Nations Resolution 69/32 on the 'No first placement of weapons in space': A step forward in the prevention of an arms race in outer space? (Elsevier, Hong Kong, Space Policy, Volume 38, Nov 2016 64-67) at 64

increasing trend in privatization of outer space, it could be valuable to include Articles to help facilitate civil law action actors borders in instances of cyberattacks.

While this is a relatively unique approach (particularly in relation to international security instruments) and one which would warrant further, dedicated study, inspiration for such policy could perhaps be drawn from the intergovernmental World Intellectual Property Organization (WIPO), which operates to promote the protection of intellectual property worldwide and to ensure administrative cooperation among the intellectual property Unions.[502] In order to attain these objectives, WIPO undertakes a number of activities, the most important of which for the present purposes are establishing norms and standards for the protection and enforcement of intellectual property rights through the conclusion of international treaties, and the facilitation of cooperation among industrial property offices concerning patent, trademark and industrial design documentation.[503] Such mechanisms,[504] which help to develop and revise legal frameworks which facilitate civil action actors borders, could potentially be adapted into a new cybersecurity instrument so as to ensure that private space actors have some means of financial recourse in the case of a cyberattack against their assets.

17. Summary

Considering the legal lacunae which exists in both outer space and cyber space law, specifically relating to the mitigation of the risk that cyber-attacks pose to outer space assets, a strong argument could be made that a new international instrument which bolsters the security

[502] Convention Establishing the World Intellectual Property Organization, July 14, 1967 and amended on September 28, 1979, No. 11846 (entered into force 26 April 1970) art. 3.

[503] World Intellection Property Organization, Summary of the Convention Establishing the World Intellectual Property Organization (accessed 28 February 2020) online: <https://www.wipo.int/treaties/en/convention/summary_wipo_convention.html>

[504] As well as the three main organs which help to enforce them, the WIPO General Assembly, the WIPO Conference and the WIPO Coordination Committee, as per *Ibid.*

of these assets is required. While the exact structure of this proposed new instrument will depend on a wide range of factors (not least which - and how many – States are involved in the negotiation), the value of a new, preferably multilateral, instrument in forming norms and reducing the chance of mistrust, misunderstandings, and miscalculations, cannot be understated.

Regardless of the Members negotiating this instrument, and whether binding provisions are able to be negotiated or not, there are certain elements which need to be considered in any new instrument. As an example, such an instrument would need to be flexible enough to respond to the rapidly-changing nature of cyber threats. It would also need to establish consensus on how jurisdiction and extradition should be established, and which acts are deserving of criminal sanctions. It may also be beneficial to explore creative solutions to this unique problem of cyber-attacks to outer space assets, particularly surrounding the facilitation of private sector civil action across borders. Such an instrument should also ensure that mechanisms are built in to ensure that States have the capacity to implement those provisions included in the instrument. Part of establishing this capacity will involve the sharing of threat information, and interaction with a wide range of parties, including industry.

CONCLUSION

The threat that cyber-attacks pose to outer space assets is severe. Such attacks are relatively inexpensive, easy, and difficult to trace – and the targets are wide-reaching, expensive, and crucial for multiple nationally-critical tasks. In that light, it is surprising to find that, apart from a range of bilateral and regional instruments, there are very few binding legal mandates to hold accountable a cyber-attack perpetrator when the attack occurs across borders (not least when it takes place against assets in the vast, unknown depths of outer space).

Reflecting this situation, protecting cyberspace and reducing its vulnerabilities to digital threats has become a fundamental element of national security strategies. While a significant number of these strategies are non-military in nature, through legislation, organizational adaptation and training, a number of States are also investigating offensive and defensive cyber capabilities of a military nature.[505] The concern that arises from this development, however, is that military cyberspace measures can lead to a cyber arms race, and a competition for "digital supremacy."[506] It is for that reason that this author believes that there is a powerful rationale for a flexible, multilateral space and cyber security regime.[507]

The world is on a geopolitical precipice. States are revealing a potentially significant vulnerability – a vulnerability which stands to be exploited by a large and unknown group of attackers with indeterminate resources. Should we not fill this existing legal lacuna, not only are we perhaps making it more likely that such attacks will take place, but we are also making it certain that such an attack will unleash a massive political backlash. As this thesis has sought to demonstrate, it is time to address these issues using every public and private law instrument that we have at our disposal, including binding or non-binding measures, and either through one large, ambitious mega-multilateral agreement or a spectrum of smaller tailored agreements. Should we not come to such a common understanding regarding acceptable State behaviour, the risk of instability and misperception will endure.

[505] J Lewis, G Neuneck, *supra* note 23 at 23.
[506] Kenneth Geers, et al, FireEye, World War C: Understanding Nation-State Motives Behind Today's Advanced Cyber-attacks (2014) online (pdf): <https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/fireeye-wwc-report.pdf>
[507] D Livingston, P Lewis, *supra* note 19 at iv.

BIBLIOGRAPHY

TREATIES

Agreement Governing the Activities of States on the Moon and other Celestial Bodies, 5 December 1979, 1363 UNTS 3 (entered into force on 11 July 1984) (Moon Agreement).

Agreement on the Rescue of Astronauts, the Return of Astronauts and Return of Objects Launched into Outer Space, 19 December 1967, 672 UNTS 119 (entered into force 3 December 1968) [Rescue and Return Agreement].

Charter of the United Nations, Oct. 24, 1945, 1 U.N.T.S. XVI [UN Charter].

Constitution and Convention of the International Telecommunications Union (as amended in 2014), 22 December 1992, UNTS 1825, No 31251.

Convention Establishing the World Intellectual Property Organization, July 14, 1967 and amended on September 28, 1979, No. 11846 (entered into force 26 April 1970)

Convention on Cyber-crime (European Treaty Series No. 185, Budapest, 23.XI.2001) online: <https://www.coe.int/en/web/conventions/search-on-treaties/-/conventions/rms/0900001680081561>

Convention on International Civil Aviation, 7 December 1944, 15 UNTS 295 (entered into force on 4 April 1947) [Chicago Convention]

Convention on International Liability for Damage Caused by Space Objects, 29 March 1972, 961 UNTS 187 (entered into force on 1 September 1972) (Liability Convention).

Convention on Registration of Objects Launched into Outer Space, 12 November 1974, 1023 UNTS 15 (entered into force on 15 September 1976) (Registration Convention).

Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), Art. 36, 8 June 1977.

Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, 27 January 1967, 610 UNTS 205 (entered into force 10 October 1967) [Outer Space Treaty or OST].

United Nations Convention on the Law of the Sea, Dec. 10 1982, 21 U.N.T.S. 1833

LEGISLATION

Australia, Security of Critical Infrastructure Act (2018)

Canada, Criminal Code (1985)

Commonwealth Consolidated Acts, Criminal Code Act 1995, online: <http://www5.austlii.edu.au/au/legis/cth/consol_act/cca1995115/sch1.html>

EU Directive on Child Exploitation (2011/93/EU)

League of Arab States Model Law (2004)

Mauritius, Computer Misuse and Cyber-crime Act (2003)

New Zealand, Crimes Act (1961)

New Zealand, Outer Space and High-altitude Activities Act (2017)

New Zealand, Terrorism Suppression Act (2002)

Telecommunications (Interception and Access) Act 1979, online: <http://classic.austlii.edu.au/au/legis/cth/consol_act/taaa1979410/>

US, Aeronautics and Space Definitions, 14 CFR § 99.3 (2004).

US, Code of Federal Regulations, 14 U.S.C. §§1030, 1037 2701

UNITED NATIONS DOCUMENTS

Analysis of the 2014 Russian-Chinese draft "treaty on the prevention of the placement of weapons in outer space, the threat or use of force against outer space objects" (PPWT), UNCD, UN Doc CD/1998 (2014).

Committee on the Peaceful Uses of Outer Space Legal Subcommittee, Status of International Agreements relating to activities in outer space as at 1 January 2019 (A/AC.105/C.2/2019/CRP.3) online: <http://www.unoosa.org/documents/pdf/spacelaw/treatystatus/AC105_C2_2019_CRP03E.pdf>

Conference on Disarmament "Analysis of the 2014 Russian-Chinese draft "treaty on the prevention of the placement of weapons in outer space, the threat or use of force against outer space objects" (PPWT) (CD/1985)" CD/1998 (2014) online: <https://documents-dds ny.un.org/doc/UNDOC/GEN/G15/007/57/PDF/G1500757.pdf?OpenElement>

Geneva Convention Relative to the Treatment of Prisoners of War, Aug. 12, 1949, 75 U.N.T.S. 135 (1949).

Group of Governmental Experts on Transparency and Confidence-Building Measures in Outer Space Activities, UNGAOR, 68th Sess, UN Doc A/68/189 (2013).

ILC Articles on Responsibility of States for Internationally Wrongful Acts with commentaries (2001), 53 UN GAOR Supp. (No. 10) at Art. 22, 31, U.N. Doc. A/56/10 (2001)

No first placement of weapons in outer space, UNGAOR, 72nd Sess, Supp No 49, UN Doc A/RES/72/27 (2017).

Prevention of an arms race in outer space, UNGAOR, 36th Sess, Supp No 51, UN Doc A/RES/36/97[C] (1981).

Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977.

United Nations, "Status of Treaties" online: United Nations Treaty Collections <https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XXIV-2&chapter=24&clang=_en>.

United Nations, "UN Manual on the Prevention and Control of Computer Related Crime" (1994) <http://216.55.97.163/wp-content/themes/bcb/bdf/int_regulations/un/CompCrims_UN_Guide.pdf>

UNODA, Report by the Chair of the Group of governmental experts on further practical measures for the prevention of an arms race in outer space, (New York, 31 January 2019) <https://s3.amazonaws.com/unoda-web/wp-content/uploads/2019/02/oral-report-chair-gge-paros-2019-01-31.pdf>

UNODA "Report of the Secretary-General on transparency and confidence-building measures in outer space activities – Replies from Governments" (2017) <https://www.un.org/disarmament/topics/outerspace/sg-report-outer-space/>

UNODC "United Kingdom National Cyber Security Strategy 2016 to 2021", <https://sherloc.unodc.org/cld/treaties/strategies/united_kingdom/gbr0005s.html?lng=en&tmpl=sherloc>

United Nations Office on Drugs and Crime, Comprehensive Study on Cyber-crime - Draft (UNODC, February 2013) online (pdf): <https://www.icao.int/cybersecurity/SiteAssets/UNODC/CYBER-CRIME_STUDY_210213.pdf>

United Nations Office on Drugs and Crime, Guidelines for the Prevention of Crime, annex to United Nations Economic and Social Council Resolution 2002/13 on Action to promote effective crime prevention (24 July 2002) online: <https://www.unodc.org/documents/justice-and-prison-reform/crimeprevention/resolution_2002-13.pdf>

UNODC "Global Program on Cyber-crime" (UNODC 2019) online: <https://www.unodc.org/unodc/en/cyber-crime/global-programme-cyber-crime.html>

United Nations General Assembly, Advancing responsible State behaviour in cyberspace in the context of international security, A/C.1/73/L.37 (11 December 2018) online: <https://digitallibrary.un.org/record/1655417>

United Nations General Assembly, Creation of a Global Culture of CyberSecurity, GA57/239 LVII A/RES/57/239 (2003) online (pdf): <https://www.oecd.org/sti/ieconomy/UN-security-resolution.pdf>

United Nations General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security, A/RES/68/243 (9 January

2014) online (pdf): <http://www.unidir.org/files/medias/pdfs/developments-in-thefield-of-information-and-telecommunications-in-the-context-of-international-security-2014-2015-a-res-68-243-eng-0-589.pdf>

United Nations General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/65/201 (July 30, 2010) online (pdf): <http://www.unidir.org/files/medias/pdfs/final-report-eng-0-189.pdf>

United Nations General Assembly, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/69/68 (June 24, 2013) online (pdf): <https://ccdcoe.org/sites/default/files/documents/UN-130624- GGEReport2013_0.pdf>

United Nations General Assembly, Twelfth United Nations Congress on Crime Prevention and Criminal Justice A/RES/65/230 (UNGA, 21 December 2010) at 42, online (pdf): <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N10/526/34/PDF/N1052634.pdf?OpenElement>

GOVERNMENTAL DOCUMENTS

Australia, Australian Attorney General's Department "National Plan to Combat Cyber-crime" at 17 (accessed 06 June 2019) online:: <https://sherloc.unodc.org/res/cld/treaties/strategies/australia/_html/national-plan-to-combat-cyber-crime_2013.pdf>

Common Market for Eastern and Southern Africa, COMESA Draft Model Bill (Gazette Vol 16, 2011) online (pdf): <https://www.comesa.int/wp-content/uploads/2016/06/2011Gazette-Vol.-16.pdf>

Commonwealth Office of Civil and Criminal Justice Reform, Model Law on Computer and Computer Related Crime, Article 9(1), (Commonwealth Secretariat, 2017) online (pdf): <http://thecommonwealth.org/sites/default/files/key_reform_pdfs/P15370_11_ROL_Model_Law_Computer_Related_Crime.pdf>

Draft African Union Convention on the Establishment of a Legal Framework Conducive to Cybersecurity in Africa (2012)

East African Community Draft Legal Framework for Cyberlaws (2008),

Economic Community of West African States "Harmonization of ICT Policies in Sub-Saharan Africa" at art. 3(ITU, 2013) online (pdf): <https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/cyber-crime_directive-explanatory_notice.pdf>

Estonia, Estonian Information System Authority position (Estonian Annual Cyber Security Assessment, 2018)

EU, Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (27 April 2016) online: <https://publications.europa.eu/en/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1/language-en>

European Commission "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace," online (pdf): <http://eeas.europa.eu/archives/docs/policies/eu-cyber security/cybsec_comm_en.pdf>

European Council, Report on Implementation of the European Security Strategy: Providing Security in a Changing World, (11 December 2008) EU document S407/08.

EUR-Lex, DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (6 Jul 2016) online: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC>

Government of Canada "Canada's Cyber Security Strategy: For a stronger and more prosperous Canada" (2010) online (pdf): <https://sherloc.unodc.org/res/cld/treaties/strategies/canada/can0003s_html/Canadas_Cyber_Security_Strategy_ENG.pdf>

HM Government "NATIONAL CYBER SECURITY STRATEGY 2016-2021" (2016) online (pdf): <https://sherloc.unodc.org/res/cld/treaties/strategies/united_kingdom/gbr0005s_html/National_Cyber_Security_Strategy_2016_to_2021_English.pdf>

Indonesia on behalf of member States of G-21 "Working paper: Prevention of an arms race in outer space (PAROS)" CD/2031 (2015)

Internet Crime Complaint Center, 2016 Internet Crime Report (Federal Bureau of Investigation, 2016) online (pdf): <https://pdf.ic3.gov/2016_IC3Report.pdf>

European Union, Launching of the EU Cyber-Resilience for Development (Cyber4D) programme in Mauritius (Mauritius , 08 Feb 2019) online: <https://eeas.europa.eu/topics/health/57808/launching-eu-cyber-resilience-development-cyber4d-programme-mauritius_en>

France, "La Stratégie nationale pour la sécurité du numérique : une réponse aux nouveaux enjeux des usages numériques," Agence nationale de la sécurité des systèmes d'information" online: <https://www.ssi.gouv.fr/actualite/la-strategie-nationale-pour-la-securite-du-numerique-une-reponse-aux-nouveauxenjeux-des-usages-numeriques/>

International Court of Justice, Legality of the Threat of Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, (Jul. 8)

Joint statement made by the Permanent Representative of Canada to the UN on behalf of Australia, Chile, Estonia, Japan, the Netherlands, New Zealand, the Republic of Korea, the United Kingdom, and Canada on Information and Telecommunications in the Context of International Security (2018) online: <https://www.international.gc.ca/world-

monde/international_relations-relations_internationales/un-onu/statements-declarations/2018-10-26-info_telecommunications.aspx?lang=eng>

League of Arab States, Arab Convention on Combating Technology Offences (21 Dec, 2010) link to text here: <https://dig.watch/instruments/arab-convention-combating-technology-offences>

Ministry of Foreign Affairs of Japan "ASEAN REGIONAL FORUM STATEMENT ON COOPERATION IN FIGHTING CYBER-ATTACK AND TERRORIST MISUSE OF CYBER SPACE" (Kuala Lumpur, 28 July 2006) Online: <https://www.mofa.go.jp/region/asia-paci/asean/conference/arf/state0607-3.html>

Netherlands, Cabinet position on encryption (April 21, 2016) online: <https://www.enisa.europa.eu/about-enisa/structure-organization/national-liaison-office/news-from-the-member-states/the-netherlands-cabinet-launched-position-on-encryption>

New Zealand Government, New Zealand's Cyber Security Strategy, 2011

New Zealand Ministry of Defence, "Defence White Paper 2010"

Organisation of American States, ADOPTION OF A COMPREHENSIVE INTER-AMERICAN STRATEGY TO COMBAT THREATS TO CYBERSECURITY: A MULTIDIMENSIONAL AND MULTIDISCIPLINARY APPROACH TO CREATING A CULTURE OF CYBERSECURITY (Resolution 2004 XXXIV-O/04, June 8, 2004) online (pdf): <https://www.oas.org/en/sms/cicte/Documents/OAS_AG/AG-RES_2004_(XXXIV-O-04)_EN.pdf>

Russia & China's Draft, "Treaty on the Prevention of the Placement of Weapons in Outer Space, the Threat or Use of Force against Outer Space Objects (Draft)," online: Nuclear Threat Initiative, <http://www.nti.org/learn/treaties-and-regimes/proposed-prevention-arms-race-space-paros-treaty/>.

Southern African Development Community (SADC) Model Law on Computer Crime and Cyber-crime (2012)

Switzerland, *Towards a "compliance-based" approach to LAWS* (Informal Working paper submitted by Switzerland, 30 March, 2016)

United Kingdom, "London Conference on Cyberspace: Chair's statement" (2 November 2011) online: <https://www.gov.uk/government/news/london-conference-on-cyberspace-chairs-statement>

United Kingdom, "Seoul Framework for and Commitment to Open and Secure Cyberspace," (Seoul Conference on Cyberspace, 2013)

United Kingdom, "UK Non Paper On Capacity Buillding -Budapest Conference" (Budapest Conference on Cybersecurity 2012, 4-5 October, 2012) online: <https://web.archive.org/web/20130530035614/http:/www.cyberbudapest2012.hu/index>

US, “2011 Report to Congress of the US-China Economic and Security Review Commission” (112 Congress, First Session, November 2011) online (pdf): <https://www.uscc.gov/sites/default/files/annual_reports/annual_report_full_11.pdf>

US, “Annual Report to Congress: Military and Security Developments Involving the People’s Republic of China 2015” Off. Secretary Def. 38-39 (Apr. 7, 2015) online: <http://www.defense.gov/Portals/1/Documents/pubs/2015_China_Military_Power_Report.pdf>.

US “International Strategy for Cyberspace” at 20 (May 2011) online (pdf): <https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf>

US, Office of the Press Secretary, “Fact Sheet: U.S.-Russian Cooperation on Information and Communications Technology Security”, (17 June 2013) online: <https://www.whitehouse.gov/the-press-office/2013/06/17/fact-sheet-us-russian-cooperationinformation-and-communications-technol.>

US, Office of the Press Secretary, “Fact Sheet: President Xi Jinping’s State Visit to the United States” (25 September 2015) online: https://www.whitehouse.gov/the-press-office/2015/09/25/factsheet-president-xi-jinpings-state-visit-united-states.

US, Office of the Press Secretary, “Joint Statement: 2016 United States-India Cyber Dialogue” (September 29, 2016) online: < https://obamawhitehouse.archives.gov/the-press-office/2016/09/29/joint-statement-2016-united-states-india-cyber dialogue>.

US, “vulnerabilities equities policy and process for the United States Government” at 1 (November 15, 2017) online (pdf): <https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF>

SECONDARY SOURCES: BOOKS

B Havel, G Sanchez “The Principles and Practice of International Aviation Law” (2014) Cambridge University Press, New York

Bin Cheng, International Responsibility and Liability for Launching Activities, XX Annals of Air and Space Law 297 (1995)

Bin Cheng, Studies in International Space Law (Oxford Scholarly Authorities on International Law, 1997).

Cohen, M. Law and Politics in Space: Proceedings of the first McGill Conference on the Law of Outer Space (Leicester University Press, Canada, 1964).

Conti, Dargahi, Dehghantanha Cyber Threat Intelligence: Challenges and Opportunities (Springer Publishing, 2018)

Frans von der Dunk, Fabio Tronchetti, eds, *Handbook of Space Law*, (Cheltenham, UK: Edward Elgar, 2015)

H.I. Touré, "The Quest for Cyberpeace" at 104 (ITU and World Federation of Scientists, 2011) online (pdf): <https://citizenlab.org/cybernorms2012/cyber peace-itu.pdf>

Hobe, Stephen et al, eds. Cologne Commentary on Space Law: in three volumes, (Köln: Carl Heymanns, 2009) at vol 1, 148

Hugo Grotius, De Jure Belli Ac Pacis. Libri Tres, Book II (1625) ¶XXIX

Ian Brownlie, Principles of Public International Law (7th ed., 2008)

Institute for Peace Research and Security Policy at the University of Hamburg, Challenges in Cybersecurity: Risks, Strategies, and Confidence Building, Institute for Peace Research and Security Policy (University of Hamburg, 2011) online (pdf): <https://www.unidir.org/files/medias/pdfs/conference-report-eng-0-373.pdf >

International Democracy Watch, League of Arab States (accessed 05 December 2019) online: <http://www.internationaldemocracywatch.org/index.php/monitored-igos/interregional-organisations/568-league-of-arab-states>

International Telecommunication Union Harmonization of ICT Policies, Legislation and Regulatory Procedures in the Caribean (2012) online (pdf): <https://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/reports/wg2/docs/HIPCAR_1-5-B_Model-Policy-Guidelines-and-Legislative-Text_Cyber-crime.pdf>

Karake-Shalhoub, Qazimi Cyber Law and Cyber Security in Developing and Emerging Economies (Edward Elgar Publishing Limited, United Kingdom 2010).

Lachs, Manfred. The Law of Outer Space: An Experience in Contemporary Law-Making, Tanja Masson-Zwaan & Stephan Hobe, eds, (Leiden: Martinus Nijhoff, 2010).

R. Weber, R. Gunnarson, "A Constitutional Solution for Internet Governance" (18 Columbia Science and Technology Law Review, 2012)

Schmitt, Michael N. et al. Tallinn Manual on the International Law Applicable to Cyber Operations, Michael Schmitt & Liis Vihul, eds, (Cambridge: Cambridge University Press, 2013) [Tallinn Manual].

Schmitt, Michael N. et al. Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare, Michael Schmitt & Liis Vihul, eds, (Cambridge: Cambridge University Press, 2017) [Tallinn Manual 2.0].

SECONDARY SOURCES: ARTICLES

A Arbatov, A Pikaev and V Dvorkin Nuclear Terrorism: Political, Legal, Strategic and Technological Aspects (Russian Politics and Law, Vol 46, No 1, Jan-Feb 2008)

A Henrikson “The end of the road for the UN GGE process: The future regulation of cyberspace” (Journal of Cybersecurity, Volume 5, Issue 1, 2019) online: <https://academic.oup.com/cybersecurity/article/5/1/tyy009/5298865>

A Seger, “India and the Budapest Convention: Why not?” (ORF Foundation, Oct 20, 2016) online: <https://www.orfonline.org/expert-speak/india-and-the-budapest-convention-why-not/>

A Soldatov, I Borogan, “Putin brings China's Great Firewall to Russia in cybersecurity pact,” (The Guardian, November 29, 2016) online: <https://www.theguardian.com/world/2016/nov/29/putin-china-internet-great-firewall-russia-cybersecurity-pact>

A Sternstein, “Cyber early warning deal collapses after Russia balks” (NextGov, 7 December 2012) online: <https://www.nextgov.com/cybersecurity/2012/12/cyber early-warning-deal-collapses-after-russia-balks/60035/>

Adam Segal, “The U.S.-China Cyber Espionage Deal One Year Later,” Net Politics (blog), the Council on Foreign Relations” (2016) online: <https://www.cfr.org/blog/us-china-cyber espionage-deal-one-year-later>

Akamai, “State of the Internet Report,” (March 2009) <https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/akamai-q1-2008-state-of-the-internet-connectivity-report.pdf>

Alex Grigsby, “Disclosing Policies on Zero-Days as a Confidence-Building Measure,” Net Politics (Council on Foreign Relations, November 18, 2014) online: <https://www.cfr.org/blog/disclosing-policies-zero-days-confidence-buildingmeasure>

Alex Grigsby, ‘The United Nations Doubles Its Workload on Cyber Norms, and Not Everyone Is Pleased’, Council on Foreign Relations (November 2018)

Alexander Cendoya, “National Cyber Security Organisation: Spain” (2016) CCDCOE, Tallinn <https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_SPAIN_092016.pdf>

Andrew Roth, “Russia and China Sign Cooperation Pacts” (New York Times, May 8, 2015) online: <https://www.nytimes.com/2015/05/09/world/europe/russia-and-china-sign-cooperation-pacts.html>

A Osula, H Roigas, “International Cyber Norms: Legal, Policy & Industry Perspectives” (CCDCOE, 2016) online (pdf): <https://ccdcoe.org/uploads/2018/10/InternationalCyberNorms_full_book.pdf>

APCO Worldwide, ‘‘China‘s 12th Five-Year Plan: How it actually works and what‘s in store for the next five years’’ (Washington, DC: December 10, 2010) online (pdf): <http://www.apcoworldwide.com/content/pdfs/chinas_12th_five-year_plan.pdf>

ARF Workshop on Proxy Actors in Cyberspace, “Co-chairs’ summary report” (Hoi An City, Viet Nam, 14–15 March 2012) online: <http://aseanregionalforum>

Arun Mohan Sukumar, “India and Russia sign cyber agreement, pushing the frontier for strategic cooperation,” (Observer Research Foundation, October 15, 2016) online: <https://www.orfonline.org/expert-speak/india-and-russia-cyber agreement/>

ASEAN Regional Forum, “About the ASEAN Regional Forum” online: <http://aseanregionalforum.asean.org/about.html>

B Acharya, K Bankston, R Schulman, A Wilson “Deciphering the European Encryption Debate: France” at 10 (Open Technology Institute, August 2017) online (pdf): <https://na-production.s3.amazonaws.com/documents/France_Paper_8_8.pdf>

B Verbeek, R Knottnerus, “The 2018 Draft Dutch Model BIT: A critical assessment” (JULY 30, 2018) online: <https://www.iisd.org/itn/2018/07/30/the-2018-draft-dutch-model-bit-a-critical-assessment-bart-jaap-verbeek-and-roeline-knottnerus/>

BBC, Cyber-attack led to Bristol Airport Blank Screens (16 Sep, 2018) online: <https://www.bbc.com/news/uk-england-bristol-45539841>

Brian Barret “The Apple-FBI Battle is Over, but the New Crypto Wars have Just Begun” (Wired, March 2016) online: <https://www.wired.com/2016/03/apple-fbi-battle-crypto-wars-just-begun/>

E Burger, G Bordacchini, *Yearbook on Space Policy 2017 – Security in Outer Space: Rising Stakes for Civilian Space Programmes* (Switzerland: Springer 2017)

C Baylon, R Brunt, D Livingstone Cyber Security at Civil Nuclear Facilities: Understanding the Risks (September 2015) Chatham House Report.

C Hurran Cyber Insiders: A Board Issue (Cyber security Review, Publication Date May 2015) online: <http://www.cybersecurity-review.com/articles/cyber insiders-a-board-issue/>

C Hurran *Cyber Insider Risk Mitigation Maturity Matrixx* (Cyber Security Review, Autumn 2016) online (pdf): <http://www.cybersecurity-review.com/wp-content/uploads/2016/11/Chris-Hurran-article-CSR-Autumn-2016.pdf>.

C Johnson, University of Glasgow “Cyber Security for Space Based Systems” <www.gla.ac.uk>

Cassese, “International Law” (2nd ed. Oxford: Oxford University Press, 2005)

CCDCOE, Basic Principles for State Policy of the Russian Federation in the Field of International Information Security to 2020 (2018) online (pdf): <https://ccdcoe.org/sites/default/files/strategy/RU_state-policy.pdf>

CCDCOE, Trends in international law for cyberspace (NATO, May 2019) online (pdf): <https://ccdcoe.org/uploads/2019/05/Trends-Intlaw_a4_final.pdf>

CERTNZ, “About us.” (accessed 16 September, 2019), online: <https://www.cert.govt.nz/about/about-us/>

Charlie Osbourne, British Airways: Cyberattack, data theft bigger than we first thought (ZDNet, October 25 2018) online: <https://www.zdnet.com/article/british-airways-cyberattack-data-theft-bigger-than-we-first-thought/>

Citizen Lab, 'Shining a Light on the Encryption Debate: a Canadian Field Guide' (The Citizen Lab and the Canadian Internet Policy & Public Interest Clinic, May 2018) online (pdf): <https://citizenlab.ca/wp-content/uploads/2018/05/Shining-A-Light-Encryption-CitLab-CIPPIC.pdf>

Civil Air Navigation Services Organisation, CANSO Cyber Security and Risk Assessment Guide ((CANSO, June 2014), online (pdf): <https://www.canso.org/sites/default/files/CANSO%20Cyber%20Security%20and%20Risk%20Assessment%20Guide.pdf>

Computer Weekly "Stuxnet: A wake-up call for nuclear cyber security attacks" W Ashford (21 October 2015) online: <www.computerweekly.com>

ComputerHope, "When was the first computer invented?" (Computer hope, February 2019) online: <http://www.computerhope.com>

D Alperovitch "Revealed: Operation Shady RAT - McAfee white paper" (2011) <http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf>

D Livingston, P Lewis Space, the Final Frontier for Cyber Security? (Chatham House, The Royal Institute of International Affairs, September 2016)

D Sanger, N Perlroth, U.S. Escalates Online Attacks on Russia's Power Grid (NY Times, Jun 15, 2019), <https://nyti.ms/2KiTwMl>

David Wallace, "Cyber Weapon Reviews under International Humanitarian Law: A Critical Analysis", NATO Cooperative Cyber Defence Centre of Excellence, Tallinn Paper 11 (2018)

Elaine Korzak, "The Next Level for Russia-China Cyberspace Cooperation?" Net Politics (blog), the Council on Foreign Relations (August 20, 2016) online: <https://www.cfr.org/blog/next-level-russia-china-cyberspace-cooperation>

Ellen Nakashima, Confidential Report Lists U.S. Weapons System Designs Compromised by Chinese Cyberspies, (Washington Post May 27, 2013) online: <http://www.washingtonpost.com/world/national-security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html>

FAI, Statement about the Karman line (FAI, November 2018) online: <https://www.fai.org/news/statement-about-karman-line>

Fox, L., Cyber security moves up the airline agenda as threats are no longer an if. (TNooz, 4 July 2016) online: <https://www.tnooz.com/article/cyber security-airlines-sita-it-trends/>

G O'Dwyer Finland Government examines centralised cyber defence (Computer Weekly, 22 May 2018) online: <https://www.computerweekly.com/news/252441613/Finland-government-examines-centralised-cyber defence>

Global Commission on the Stability of Cyber Space, "BRIEFINGS FROM THE RESEARCH ADVISORY GROUP" at 11, (New Delhi, November 2017) online (pdf): <https://cyberstability.org/wp-content/uploads/2017/12/GCSC-Briefings-from-the-Research-Advisory-Group_New-Delhi-2017.pdf>

Global Sign "Six Cybersecurity tools and services every business needs" (Globalsign, 28 August 2018) online: <https://www.globalsign.com/en/blog/six-cybersecurity-tools-and-services-every-business-needs/>

Grees, Kenneth, "Cyber War in Perspective: Russian Aggression against Ukraine" (2016) CCDCOE, Tallinn <https://ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_full_book.pdf>

Greegs, Kenneth et al, FireEye, World War C: Understanding Nation-State Motives Behind Today's Advanced Cyber-attacks (2014) online (pdf): <https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/fireeye-wwc-report.pdf>
Group of Twenty "G20 Leaders Communiqué," online: <http://www.mofa.go.jp/files/000111117.pdf>

H Liu, F Tronchetti *United Nations Resolution 69/32 on the 'No first placement of weapons in space': A step forward in the prevention of an arms race in outer space?* (Elsevier, Hong Kong, Space Policy, Volume 38, Nov 2016 64-67)

Iain Thomson, "Germany, France lobby hard for terror-busting encryption backdoors – Europe seems to agree" (The Register, February 2017) online <https://www.theregister.co.uk/2017/02/28/german_french_ministers_breaking_encryption/>.

ICAO, *Annex 17 to the Convention on International Civil Aviation: Security: Safeguarding International Aviation Against Acts of Unlawful Interference* (ICAO, 10th Edition, April 2017) at 4.9, online (pdf): <http://dgca.gov.in/intradgca/intra/icao%20annexes/an17_cons.pdf>

ICAO, Civil Aviation Cybersecurity Action Plan (ICAO, Dec 2014) online (pdf): <https://www.icao.int/cybersecurity/SiteAssets/ICAO/Civil%20Aviation%20Cybersecurity%20Action%20Plan%20-%20SIGNED.pdf>

ICAO "Civil Aviation Cybersecurity Information Repository", online: <https://www.icao.int/cybersecurity/Pages/default.aspx>

ICRC, *A Guide to the Legal Review of New Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977* (International Committee of the Red Cross Geneva, January 2006)

Ihsan Burak Tolga, "Principles of Cyber Deterrence and the Challenges in Developing a Credible Cyber Deterrence Posture", NATO Cooperative Cyber Defence Centre of Excellence, Tallinn 2018 (2018)

Institute for Defence and Government Advancement, “5th Annual Cyber Security For Defence” (accessed 10 August 2019) website: <https://www.idga.org/events-cybersecurityfordefence>

International Air Transport Association, Cyber Security Fact Sheet (IATA, December 2018), online (pdf): <https://www.iata.org/pressroom/facts_figures/fact_sheets/Documents/fact-sheet-cyber security.pdf>

International Atomic Energy Agency Computer Security at Nuclear Facilities (IAEA Nuclear Security Series No 17, Vienna, 2011)

International Organization for Standardization ISO/IEC 27001 (Interdisziplinarer Normenbereich Sectur interdisciplinaire de normalisation, 2013) online (pdf): <https://trofisecurity.com/assets/img/iso27001-2013.pdf>

INTERPOL Third INTERPOL Symposium on International Fraud (Paris 11-13 December 1979)

Israel Aerospace Industries “Cyber Solutions: End-to-End Cyber Solutions” <http://www.iai.co.il>

ITU, Collection of the basic texts adopted by the Plenipotentiary Conference, at 523 (ITU Publications, 2019) online (pdf): <http://search.itu.int/history/HistoryDigitalCollectionDocLibrary/5.22.61.en.100.pdf>

ITU, Global Cybersecurity Agenda (GCA) (accessed 19 September 2019) online (pdf): <www.itu.int/osg/csd/cybersecurity/gca/new-gca-brochure.pdf>

ITU, Global Cybersecurity Index (GCI) 2018 at 18 (ITU Publications, 2018) online (pdf): <https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf>

J. E. S. Fawcett “Outer Space: New Challenges to Law and Policy” (1984) Clarendon Press, Oxford

J Jakóbowski “Chinese-led Regional Multilateralism in Central and Eastern Europe, Africa and Latin America: 16 + 1, FOCAC, and CCF” (2018) Journal of Contemporary China, Volume 27, Issue 113, 659-673)

J Kagan, Bilateral Trade (Investopedia, May 24 2019) online: <https://www.investopedia.com/terms/b/bilateral-trade.asp>
J Kirk, “Despite Controversy, Cyber-crime Treaty Endures” (PCWorld, 21 November 2011) online: <https://www.pcworld.com/article/244407/despite_controversy_cyber-crime_treaty_endures.html>

J Nye Jr Nuclear Lessons for Cyber Security? (Strategic Studies Quarterly 5(4): 18-38, Winter 2011)

J Lewis, G Neuneck, The Cyber Index: International Security Trends and Realities (New York and Geneva: United Nations Institute for Disarmament Research, 2013) online (pdf): <http://www.unidir.org/files/publications/pdfs/cyber index-2013-en-463.pdf>

Jeff Foust, Blue Origin plans to start selling suborbital spaceflight tickets next year (Spacenews, 21 June 2018) online: <https://spacenews.com/blue-origin-plans-to-start-selling-suborbital-spaceflight-tickets-next-year/>

L Daniel, Digital Forensics for Legal Professionals: Understanding Digital Evidence from the Warrant to the Courtroom (1st Ed., Syngress, 2011)

L Johnstone, Euronews answers: The Council of Europe turns 70, but what does it do? (euronews, 02 October, 2019) <https://www.euronews.com/2019/10/01/euronews-answers-the-council-of-europe-turns-70-but-what-does-it-do>

Le Monde. (2018). Les orientations diplomatiques d'Emmanuel Macron (27 July 2018) sécurité en Europe et crise humanitaire en Syrie. <https://www.lemonde.fr/international/article/2018/ 08/27/europe-syrie-libye-macron-devoile-sa-feuille-de-route-diplomatique_5346644_3210.html>

L Napoleoni Modern Jihad: Tracing the Dollars Behind the Terror Networks (Pluto Press, London, 2003)

Leslie Meredith, Malware implicated in fatal Spanair plane crash (NBCNews, 20 August 2010) online: <http://www.nbcnews.com/id/38790670/ns/technology_and_science-security/t/malware-implicated-fatal-spanair-plane-crash/#.XLemyOi6O70>

M Azriel "Emergence of Cyber Security Products for Space Systems" (October 5, 2012) <www.spacesafetymagazine.com>

M Papa, "Regulation (EU) 2016/679: how the European personal data protection landscape will change" (European Union, May 31, 2016) online: <https://www.lexology.com/library/detail.aspx?g=27ae467a-e2ed-4efc-ba4d-16d74c95e661>

Marie Baezner, "Cybersecurity in Sino-American Relations" (Center for Security Studies, No. 224, April 2018) online (pdf): <https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse224-EN.pdf>

Microsoft, "A Digital Geneva Convention" online (pdf): <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW67QH>

Microsoft, "From Articulation to Implementation: Enabling progress on cybersecurity norms," online (pdf): <https://mscorpmedia.azureedge.net/mscorpmedia/2016/06/Microsoft-Cybersecurity-Norms_vFinal.pdf>

Mikk Raud, China and Cyber: Attitudes, Strategies, Organisation (CCDCOE, Tallinn, 2016) <https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_CHINA_092016_FINAL.pdf>

Morgan “2019 Cybersecurity Almanac: 100 Facts, Figures, Predictions and Statistics” (06 Feb 2019, New York) online: <https://cybersecurityventures.com/cybersecurity-almanac-2019/>

N Lord, What are Indicators of Compromise (Digital Guardian, September 11, 2018) online: <https://digitalguardian.com/blog/what-are-indicators-compromise#:~:targetText=Indicators%20of%20compromise%20(IOCs)%20are,on%20a%20system%20or%20network.%E2%80%9D>

NATO Cooperative Cyber Defence Centre of Excellence, “About”, www. ccdcoe.org.

N Weiss, “Cyber Security of the Space Eco-System” (2017 Space Security Conference, United Nations Office at Geneva, Switzerland, 20-21 April 2017)

Nuclear Threat Initiative “Conference on Disarmament” (April 27, 2017) online: <http://www.nti.org/learn/treaties-and-regimes/conference-on-disarmament/>

OAS, “Cyber security program” online: <www.oas.org/en/sms/cyber>

OAS, “Press Release: OAS Presents Mobile Simulation Laboratory for Cyber-attack Response Exercises” (August 31, 2012) online: <http://www.oas.org/en/media_center/press_release.asp?sCodigo=E-298/12>

Olga Razumovskaya, ‘Russia and China Pledge Not to Hack Each Other,’ (Wall Street Journal, May 8, 2015) online: <http://blogs. wsj.com/digits/2015/05/08/russia-china-pledge-to-not-hack-each-other/>

Organisation for Economic Co-operation and Development, “Global Forum on Digital Security for Prosperity” (accessed 10 August 2019) online: <https://www.oecd.org/internet/global-forum-digital-security/about/>

OSCE, Astana Declaration of the OSCE Parliamentary Assembly and Resolution Adopted at the Seventeenth Annual Session (Organization for Security and Co-operation in Europe, Seventeenth Annual Session, Astana, 29 June to 3 July 2008) online (pdf): <https://ccdcoe.org/sites/default/files/documents/OSCE-080703-AstanaDeclarationandResolutions.pdf.>

OSCE, Belgrade Declaration of the OSCE Parliamentary Assembly and Resolution Adopted at the Twentieth Annual Session (Organization for Security and Co-operation in Europe, Twentieth Annual Session, Belgrade, 6-10 July 2011) online (pdf): <https://www.oscepa.org/documents/all-documents/annual-sessions/2011-belgrade/declaration-4/3024-belgrade-declaration-eng/file>;

OSCE, Conference on Security Co-operation in Europe: Final Act (Organization for Security and Co-operation in Europe, Conference on Security Co-operation, Helsinki, 1975) online: <https://www.osce.org/mc/39501?download=true>

OSCE, Oslo Declaration of the OSCE Parliamentary Assembly and Resolution Adopted at the Nineteenth Annual Session (Organization for Security and Co-operation in Europe,

Nineteenth Annual Session, Oslo, 6-10 July 2010) online (pdf): <https://ccdcoe.org/sites/default/files/documents/OSCE-100710-OsloDeclarationandResolutions.pdf>

OSCE, Permanent Council decision No. 1039, Development of Confidence Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies, PC.DEC/1039 (26 April 2012) online: <http://www.osce.org/pc/90169?download=true>

Otani, Oskami, Kahtake, "Dual-Use Concept on Civil and Defense Uses of Outer Space" at 2 (Japan Society for Aeronautical and Space Sciences and ISTS. January 2012)

P Tzeng, "The State's Right to Property Under International Law" (Yale Law Journal, Vol. 125, Issue 6, 2016) 1548-1819, online: <https://www.yalelawjournal.org/comment/the-states-right-to-property-under-international-law>

Poloalto Networks "What is Cybersecurity?" <www.paloaltonetworks.com>

PriceWaterhouseCoopers, 2015 Global airline CEO survey, Getting clear of the clouds: Will the upward trajectory continue? (PWC, Dec. 2015), online (pdf): <http://www.pwc.com/us/en/industrial-products/publications/assets/pwc_2015_global_airline_ceo_survey.pdf>

PriceWaterhouseCoopers, Aviation perspectives 2016 special report series: Cybersecurity and the airline industry – Part 1 of 4: Introduction (PWC, 2016), online (pdf): <https://www.pwc.com/us/en/industrial-products/publications/assets/pwc-airline-industry-perspectives-cybersecurity.pdf>

Privacy Shield framework, "Privacy Shield Overview" (accessed 16 September 2019) online: <https://www.privacyshield.gov/Program-Overview>

Raymond Zhong, Cathay Pacific Data Breach Exposes 9.4 Million Passengers (New York Times, 25 Oct 2018) online: <https://www.nytimes.com/2018/10/25/business/cathay-pacific-hack.html>

Reaching Critical will, Conference on Disarmament GE 02-42978 (CD/1679) (2002) <http://www.reachingcriticalwill.org/images/documents/Resources/Factsheets/paros/CD1679.pdf>

RT Logic "About Us" (2017) <www.rtlogic.com>

S Lohr, "U.S. Moves to Ban Huawei From Government Contracts" (NY Times, 7 August. 2019) online: <https://www.nytimes.com/2019/08/07/business/huawei-us-ban.html>

S. Myrli, NATO and Cyber Defence, para 45 (NATO, 173 DSCFC 09 E bis, 2009)

Schmitt et. Al. "The Law of Cyber Targeting" at 20 (CCDCOE, Tallinn Paper No. 7, 2015) online (pdf): <https://ccdcoe.org/uploads/2018/10/TP_07_2015.pdf>

Shanghai Cooperation Organization, "Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International

Information Security" (61st plenary meeting, 2 December 2008) online: <http://media.npr.org/assets/news/2010/09/23/cyber_treaty.pdf>

Smith, Marcia. "NASA's FY2020 Budget Request." (13 June 2019) online: <https://spacepolicyonline.com/fact-sheets-reports/>

Tech accord, "CYBERSECURITY TECH ACCORD" online: <https://cybertechaccord.org/accord/>

Union of Concerned Scientists, "UCS Satellite Database" online: <https://www.ucsusa.org/>

USTelecom. "USTelecom Cybersecurity Policy Forum: National Cyber Policy Guidance", (accessed 10 August) online: <https://www.idga.org/events-cybersecurityfordefence>

V Boulanin *Implementing Article 36 Weapon Reviews in the Light of Increasing Autonomy in Weapon Systems* (SIPRI Insights on Peace and Security, No. 2015/1, November 2015)

V Radunovic, At the table with the Paris Call for Trust and Security in Cyberspace (19 December 2018) online: <https://www.diplomacy.edu/blog/table-paris-call-trust-and-security-cyberspace>

Weiss, N "UNIDIR Space Security Conference 2017 Celebrating the Outer Space Treaty: 50 Years of Space Governance and Stability Conference Report" (20-21 April, 2017) <http://www.unidir.org/files/publications/pdfs/unidir-space-security-2017-en-685.pdf>

World Intellection Property Organization, Summary of the Convention Establishing the World Intellectual Property Organization (accessed 28 February 2020) online: <https://www.wipo.int/treaties/en/convention/summary_wipo_convention.html>

Y Lipkin, A Shlomo, A Paz, D Menaker, G Mizrahi, N David Critical Infrastructure and Operational Technology Security (Cyber Security Review, Delta Business Media, Autumn 2015)

Zahra Dsouza Are Cyber Security Incident Response Teams (CSIRTs) Redundant or Can They Be Relevant to International Cyber Security? 69.3 (January 2018)