The Developing Concept of Sovereignty

Considerations for Defence Operations in Cyberspace and Outer Space

June 2021

Dan Jerker B. Svantesson
Rebecca Azzopardi
Wendy Bonython
Jonathan Crowe
Steven Freeland
Samuli Haataja
Danielle Ireland-Piper
Nathan Mark

The Developing Concept of Sovereignty: Considerations for Defence Operations in Cyberspace and Outer Space

June 2021

© Dan Jerker B. Svantesson; Rebecca Azzopardi; Wendy Bonython; Jonathan Crowe; Steven Freeland; Samuli Haataja; Danielle Ireland-Piper; Nathan Mark. 2021

All rights reserved. Subject to the terms of the Copyright Act, no part of this publication may be reproduced, or stored in a retrieval system, or transmitted, in any form or by any means (photocopying, electronic, mechanical, recording, or otherwise) without the prior written permission of the copyright holder.

Published by the Technology and Jurisdiction Research Team
Faculty of Law
Bond University
Queensland, 4229,
AUSTRALIA.
Phone +61 7 5595 2058
Webpage:
https://bond.edu.au/researchers/research-strengths/faculty-research-profiles/law/technology-and-jurisdiction

Email: lawresearch@bond.edu.au

National Library of Australia Cataloguing-in-Publication entry:

Authors:	Svantesson, Dan Jerker B.; Azzopardi, Rebecca; Bonython, Wendy; Crowe, Jonathan; Freeland, Steven; Haataja, Samuli; Ireland-Piper, Danielle; Mark, Nathan
Title:	*The Developing Concept of Sovereignty: Considerations for Defence Operations in Cyberspace and Outer Space* / Dan Jerker B. Svantesson; Rebecca Azzopardi; Wendy Bonython; Jonathan Crowe; Steven Freeland; Samuli Haataja; Danielle Ireland-Piper; Nathan Mark.
Edition:	1st ed
ISBN:	978-0-6452396-0-7
Subjects:	Law; Warfare & Defence

Foreword

by MAJGEN (Retd) Marcus Thompson AM PhD

This Report provides important insights into an important topic, and I wish to start by congratulating the authoring team on their excellent work. The Report addresses the topic of sovereignty, and in doing so, it takes particular account of sovereignty in the cyber and outer space domains – two domains of great significance for Australia's national interests. It is written with commendable clarity and should serve the needs of strategic planners in Defence as well as strategic policy planners in government more broadly.

The Report is extremely timely since the concept of 'sovereignty' has recently gained new life in Australia and around the world not least in the cyber context. Increased tensions with China, a constant flow of fake news, frequent references to cyber-attacks conducted by sophisticated State actors, and public announcements on foreign espionage have placed sovereignty front and centre in the Australian psyche. We are in an era of cyber spies and cyber warriors, and with near-universal dependence on digital information and electronic devices, cybersecurity – both on our planet and in space – has become critically important for society as a whole.

The Report makes several valuable recommendations. For example, it observes that Australia must work with its partners and allies to steer the direction of definitions and delineations in international law, including in relation to the centrally important concept of sovereignty. This engagement must, as the Report argues, be broad and multifaceted and include all current formative debates about the concept of sovereignty and its related concepts.

It also emphasises the necessity of maintaining Australia's commitment to a rules-based international order, and that ongoing militarisation and threatened weaponisation of space represents a significant national security challenge for Australia and other nations. Further, it notes that the territorial conception of sovereignty is challenged by recent developments. These include threats to sovereignty, such as global terrorism and cyber-attacks, which do not follow territorial boundaries. States can no longer preserve their internal sovereignty solely, or even primarily, by policing their geographical borders.

The Report follows a logical structure. The introductory chapter considers literature pertinent to the debate to show why it is important for Defence and policy planners to considering sovereignty in a Defence context. Chapter 2 of the Report provides readers with a critical analysis of the concept of sovereignty, how it has developed and how the concept may be constructed, informed by recent and ongoing critical debates. Chapter 3 considers how the concept of sovereignty may apply in the emerging domain of cyberspace, while Chapter 4 considers sovereignty's application to the space domain. Chapter 5 provides some concluding thoughts and recommendations for future consideration. I strongly encourage readers to consider the complete Report, but note that each chapter may be considered as a standalone document for members of an interest-specific audience.

MAJGEN (Retd) Marcus Thompson AM PhD retired from the Australian Army in 2021. His career spanned 34 years and culminated in his appointment as the inaugural head of the Australian Defence Force's Information Warfare Division. In this role, Marcus saw first-hand how nation States are seeking to leverage the cyber and space domains independently or in support of operations in the traditional air, land and sea domains. Since leaving the army in January 2021, he has founded an independent advisory focused on improving cybersecurity and developing sovereign Australian capability, working with a number of Australian companies including Macquarie Telecom Group, Penten and ParaFlare.

Table of Contents

Contributors ***v***

Acknowledgements ***ix***

Executive Summary ***x***

CHAPTER 1: Introduction **1**
The developing concept of sovereignty and its defence application, particularly in cyberspace and outer space **3**

Why it matters: Defence policy on the space and cyber domains **4**

CHAPTER 2: The concept of sovereignty ***11***
The concept of sovereignty 12
Sovereignty in the defence context 12
Sovereignty in legal theory 14
Sovereignty in international law 14
Sovereignty in international relations 16

Conceptual issues and debates 17
Sovereignty as inherent or contested 17
Sovereignty as right, privilege, power or immunity 18
Sovereignty as a rule or a principle 18

Refining the concept of sovereignty 19
Sovereignty as a practice 19
Sovereignty as a functional concept 19
Sovereignty as a bundle concept 20

Implications for the defence context 21
Sovereignty and defence coordination 21
A pragmatic pluralist framework 22

CHAPTER 3: The concept of sovereignty in the cyber domain ***23***
Background **24**
Internet governance and regulation 24
United Nations processes and international law 25
Sovereignty in cyberspace **27**
Overview of the debate 27
The current position of States on sovereignty 30
The non-intervention principle 33
The prohibition on the use of force 36
Examples of specific activities:
Disinformation operations 38
Cyber espionage 41
Cyber-attacks 42

New and emerging concepts of sovereignty 43

Concluding remarks regarding sovereignty in the cyberspace context 45

CHAPTER 4: The relevance for Defence of the developing concept of sovereignty in the space domain ***46***

Background 47
Sovereignty in outer space 54
Space as res communis 54
The delineation dilemma: where does space start? 54
Australia's legislative position 57
Sovereign rights in space 61
Sovereign rights over nationals and space objects 61
Sovereign rights to natural resources 62
Sovereign obligations in space 63
Defence implications of sovereignty in outer space 64
Weapons testing and development 64
Competition for natural resources 66
Information and intelligence gathering 69
Conclusion: A strategic role for Australia in space 71

CHAPTER 5: Concluding remarks ***72***

Contributors

Professor Dan Jerker B. Svantesson is based at the Faculty of Law, Bond University. He is an Associated Researcher at the Swedish Law & Informatics Research Institute, Stockholm University (Sweden), and a Visiting Professor at Masaryk University (Czech Republic). Professor Svantesson specialises in international aspects of the IT society, a field within which he has published a range of books, reports, and articles, and given presentations in Australia, Asia, North America and Europe. Professor Svantesson was an ARC Future Fellow (2012-2016) and was awarded the Vice Chancellor's Award Research Excellence in 2016. He has been identified as the field leader in "Technology Law" in The Australian RESEARCH magazine three years in a row (2018, 2019 and 2020).

Dan Jerker B. Svantesson

Rebecca Azzopardi is a PhD candidate at Bond University. Her research is in the area of data law and considers the breadth of data collection and sharing in Australia and the UK for the purposes of national security, with a focus on border protection. Rebecca is a Principal Legal Officer in the Commonwealth government, with expertise in data and information law, privacy and secrecy and has taught constitutional and administrative law at Bond University. She also assisted the Internet & Jurisdiction Policy Network in the production of its inaugural 2019 *Global Status Report* on cross border legal challenges on the Internet, leading interviews with stakeholder experts and providing research support.

Rebecca Azzopardi

Wendy Bonython is an Associate Professor in the Faculty of Law at Bond University. She has post graduate qualifications in law and molecular medicine, and is an admitted legal practitioner. Prior to entering academia she worked for the Commonwealth government in the Department of Defence. Her research and teaching encompasses the intersections of law, ethics and regulation, and technology. She is currently the legal member of the Defence Department of Veterans' Affairs Human Research Ethics Committee.

Wendy Bonython

Jonathan Crowe is Professor of Law at Bond University. He is the author or editor of nine books and more than 100 scholarly book chapters and journal articles, primarily on legal philosophy, ethical theory and public law. His recent books include *Mediation Ethics: From Theory to Practice* (Edward Elgar, 2020) (co-authored with Rachael Field), *Natural Law and the Nature of Law* (Cambridge University Press, 2019) and the *Research Handbook on Natural Law Theory* (Edward Elgar, 2019) (co-edited with Constance Youngwon Lee). He is a founding Co-Director of Rape and Sexual Assault Research and Advocacy, an Australia-wide initiative working to shape community responses to sexual violence. He is also the current joint President of the Australian Dispute Resolution Research Network and a former President of the Australasian Society of Legal Philosophy. He co-edits the *Journal of Legal Philosophy* with Hillary Nye.

Jonathan Crowe

Steven Freeland is Emeritus Professor of International Law at Western Sydney University, where he was previously the Dean of the School of Law, and Professorial Fellow at Bond University. He also holds Visiting or Adjunct positions at various other Universities/Institutes in Copenhagen, Vienna, Toulouse, Hong Kong, Montreal, Kuala Lumpur, Vancouver and London. Prior to becoming an academic, he had a 20-year career as an international commercial lawyer and an investment banker. He is a Member of the Australian Space Agency Advisory Board and has been an advisor to the Australian, New Zealand, Norwegian and several other Governments on issues relating to national space legislative frameworks and policy. He has represented the Australian Government at Committee on the Peaceful Uses of Outer Space (UNCOPUOS) meetings and has also been appointed by UNCOPUOS to co-chair multilateral discussions on the exploration, exploitation and utilisation of space resources, which will take place in June 2021. He has also been a Visiting Professional within the Appeals Chamber at the International Criminal Court, and a Special Advisor to the Danish Foreign Ministry in matters related to the International Criminal Court. He is a Co-Principal of specialised space law firm Azimuth Advisory and is also a Director of the International Institute of Space Law, and a Member of the Space Law Committee of the International Law Association and the Space Law and War Crimes Committees of the International Bar Association. In addition to co-Editing the Annotated Leading Cases of International Criminal Tribunals book series, he also sits on the Editorial Board / Advisory Board of a number of internationally recognised academic journals.

Steven Freeland

Samuli Haataja is a lecturer at Griffith Law School, Griffith University. His research explores law and emerging technologies with a focus on cyberspace and public international law. He published his book *Cyber Attacks and International Law on the Use of Force: The Turn to Information Ethics* with Routledge in 2019, and he has published in various international law and technology journals. He is also a member of the Program on the Regulation of Emerging Military Technologies (PREMT) and the Institute of Electrical and Electronics Engineers Society on Social Implications of Technology (IEEE SSIT).

Samuli Haataja

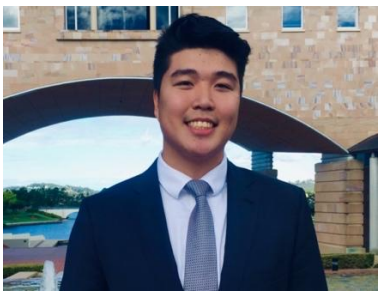
Danielle Ireland-Piper is Associate Professor at Bond University. Danielle has an LLM from the University of Cambridge, where she was a Chevening Scholar, and a PhD from the University of Queensland. She is the author of *Accountability in Extraterritoriality: A Comparative and International Law Perspective* (Edward Elgar, 2017) and *Extraterritoriality in East Asia: Extraterritorial Criminal Jurisdiction in China, Japan, and South Korea* (Edward Elgar, 2021), as well as book chapters and journal articles on various aspects of international and constitutional law. Danielle has previously served in various government roles, including at both federal and state levels, and also practiced law in the private sector.

Danielle Ireland-Piper

Nathan Mark is a Master of Laws Candidate at Bond University. His research looks at the technological and jurisdictional challenges associated with obtaining evidence from transnational digital sources as part of criminal proceedings in the Australian federal jurisdiction. Nathan is also employed as the Principal Solicitor at Aspera Legal & Consulting and has worked as a sessional law lecturer. Prior to embarking on a legal career, Nathan served in the Australian Regular Army for 19 years where he predominately served as a Royal Australian Corps of Signals Officer with the 3rd Combat Signal Regiment and The Special Air Service Regiment.

Nathan Mark

Research assistants



Elijah recently graduated with a Bachelor of Laws (Hons) from Bond University. He is now pursuing a career in international arbitration practice. Elijah has an interest in the procedural aspects of international dispute settlement.

Elijah Png

Holli is a PhD candidate at Bond University. Her research focuses on the role of Access to Justice initiatives in supporting the Rule of Law. Holli also holds various roles at Bond as an Assistant Teaching Fellow, Semester Tutor in Critical Thinking and Communication, and Senior Research Assistant. Holli is author of 'International law and terrorism: the case of ISIS' in *Handbook of Terrorism and Counter Terrorism Post 9/11* (Edward Elgar, 2019), 'Does International Law Apply to the Islamic State?' (Geneva Centre for Security Policy, 2017), in addition to articles regarding domestic law. Before commencing her PhD, Holli gained practical experience in law as a Judge's Associate at the Supreme Court of Queensland, and later as a lawyer at Legal Aid Queensland.

Holli Edwards

Acknowledgments

Much of this Report was written on the lands of the Yugembeh people. To that end, we acknowledge and pay respects to the people of the Yugembeh language group and to elders past and present.

This research was supported by the Australian Government through a grant by the Australian Department of Defence. The views expressed herein are those of the authors and are not necessarily those of the Australian Government, the Australian Department of Defence, or the universities or other institutions the authors are affiliated with.

We are grateful to the Faculty of Law and the Office of Research Services at Bond University for their support. In particular, we thank Tonya Roberts, Research Development Manager, for her kind assistance.

We also acknowledge and thank our research assistants, Jane Andrews, Holli Edwards, and Elijah Png, for their excellent work.

Finally, given this Report was written in 2020 and 2021, we acknowledge and thank the health and other first responder and frontline workers worldwide who have helped keep us safe during these trying times.

Executive summary

The cyber and space domains are of significance for Australia's national interests. In addition, the cyber and space domains are important facilitators of Australia's defence capabilities in the traditional maritime, air, and land domains.

The concept of 'sovereignty' has a range of different definitions. Those definitions are often imprecise and partly context dependent. Sovereignty has a particular resonance in the defence context. In that context, sovereignty is tied to a State's defensive capabilities. States commonly justify investment in defensive capabilities as linked to securing national interests and thus maintaining sovereignty. Defensive sovereignty is also often linked to the concept of self-reliance in national security.

Australia must maintain its commitment to a rules-based international order. And the definition and delineation of key concepts, such as 'sovereignty', is of great strategic importance. A pragmatic but principled approach to sovereignty will best serve Australia's strategic interests in contested areas like cyberspace and outer space jurisdiction.

Australia must work with its partners and allies to steer the direction of definitions and delineations in international law, including in relation to the centrally important concept of sovereignty. This engagement must be broad and multifaceted and include all current formative debates about the concept of sovereignty and its related concepts.

Uncertainty about the thresholds for activities that could trigger a military response in space or cyberspace undermines predictability and Australia's ability to respond to potential infringements of its national interests in these domains, thus undermining Australia's capacity to defend its own interests and those of its allies.

In parallel to the mentioned need for international norm-setting within the commitment to a rules-based international order, Australia must work on formulating a coherent understanding of sovereignty in the context of the space and cyberspace domains for its own purposes. While this internal formulation will need to be aligned with international developments, the internal formulation has become even more pressing in the light of increasingly public ambitions to develop offensive cyberspace capabilities.

Both cyberspace and outer space are dual use environments with both State and non-State actors present and both military and civilian applications. While cyberspace is predominantly regulated by general international law, activities in outer space are subject to important international agreements.

Article IV of the Outer Space Treaty makes clear that '[t]he Moon and other celestial bodies shall be used by all States Parties to the [Outer Space] Treaty exclusively for peaceful purposes'. However, the current (geo)political momentum appears to be directed towards an even greater incorporation of satellite technology in outer space as an integral part of the conduct of warfare. The twin policy for Australia of ensuring access to space through strategic alliances with certain space-faring nations, whilst also developing further sovereign space capability in specific areas, is essential to Australian national security.

Australia is increasingly subject to aggression in cyberspace. This aggression comes in multiple forms and is directed at both civilian and military targets. Australia needs to continue developing both its defensive and offensive capabilities in cyberspace. Given how interlinked civilian and military assets are in cyberspace, this must be done adopting a 'total defence' ('whole-of-society') approach under which civilian and military assets work together against cyber-attacks on Australian interests.

Concepts including 'data sovereignty' and 'technological sovereignty' are emerging, and the exact role of sovereignty is in debate. The current debate about sovereignty in the cyber context largely revolves around the circumstances under which a State's sovereignty is violated by the cyber activities of another State. This debate can be generalised as involving two different positions: the 'sovereignty as a rule' approach and the 'sovereignty as a principle' approach. Most States that have expressed their legal position have adopted the view that sovereignty operates as a rule of international law that can be violated by cyber operations. However, the threshold at which this occurs remains disputed. States officially articulating their positions on matters such as sovereignty in cyberspace can help develop shared understandings and potentially lead to the development of customary international law. As noted, Australia must actively engage in this.

Future research, building on the work of this Report, may usefully explore (a) the interaction and relationship between cyber and outer space, and (b) the roles of cyber and outer space in hybrid 'grey zone' conflicts.

CHAPTER 1

Introduction

CHAPTER 1: Introduction

The developing concept of sovereignty and its defence application, particularly in cyberspace and outer space 3

Why it matters: Defence policy on the space and cyber domains 4

The 2020 Strategic Update[1] and the 2020 Force Structure Plan[2] identified the management of cyber and information, and space, capabilities as strategically important, alongside maritime, air, and land capabilities. Reliance on spatial and cyberspatial networked technologies underpins almost every aspect of our lives, from the most benign civilian communication technologies through to the most advanced military defensive systems.

Despite being critical enablers of human security and despite developing rapidly, cyberspace and space are also critical vulnerabilities. Malicious exploitation of space and cyberspace technologies yields massive potential for disruption and destabilisation while avoiding traditional military conflict-dubbed 'grey zone' activities.

The 2020 Strategic Update also reaffirmed Australia's commitment to a rules-based international order, identifying pressure on the system of rules and norms governing use of global commons including space and cyberspace as a strategic threat. The Strategic Update expressly noted uncertainty about the 'thresholds for activities that could trigger a military response' in space or cyberspace due to the absence of recognised jurisdictional boundaries or limits associated with conceptions of sovereignty that exist in the established domains of land, air and sea. This uncertainty challenges our ability to predict and respond to potential infringements of our national interests in these domains, undermining our capacity to defend our own interests and those of our allies.

This Report explores how the concept of sovereignty, which forms part of the rules-based global order, applies within the emerging critical global domains of space and cyberspace.

KEY POINT:

"...uncertainty challenges our ability to predict and respond to potential infringements of our national interests in these domains, undermining our capacity to defend our own interests and those of our allies."

[1] Department of Defence, *2020 Defence Strategic Update* (1 July 2020) <https://www1.defence.gov.au/sites/default/files/2020-11/2020_Defence_Strategic_Update.pdf> ('*2020 Defence Strategic Update*').
[2] Department of Defence, 2020 *Force Structure Plan* (1 July 2020) <https://www1.defence.gov.au/strategy-policy/strategic-update-2020>.

The developing concept of sovereignty and its defence application, particularly in cyberspace and outer space

Sovereignty delineates the scope of legitimate State activity, including in cyber and space environments. Both cyberspace and space vulnerabilities were identified as threats to the strategic environment in the 2016 Defence White Paper.[3] Concepts including 'data sovereignty' and 'technological sovereignty' are emerging, and the exact role of sovereignty is in debate. For example, is sovereignty merely an underlying principle or is it something that can be violated in its own right? This Report analyses conceptions of sovereignty in the cyber and space strategic environments, to inform understanding of legitimacy of actions by and against Australia within those environments.

This Report is the culmination of a research project funded by the 2020 Department of Defence Strategic Policy Grants Program. The project sought to examine the defence implications that the concept of sovereignty has on activities undertaken in the space and cyberspace domains. The Report sets out the contested conceptions of the core international legal principle of sovereignty. It identifies existing tensions within understandings of sovereignty in its application to traditional territorial disputes between States. These include whether sovereignty is itself a national interest, breach of which gives rise to State responsibility; or whether it is merely an underlying principle of other rules, breach of which enlivens other national interests that can be violated legitimising a defensive response.

The Report then explores the applicability of existing conceptions of sovereignty to the emerging critical domains of space and cyberspace, with a view to informing Defence's conceptualisation of the margins of those domains in order to establish the thresholds for incursion which may trigger a military response.

It is envisaged that this timely analysis will provide readers with a legally informed understanding of sovereignty against which the legitimacy of activities – including activities undertaken by Australian actors – in cyberspace and space can be analysed, reducing potential for misunderstandings and conflict.

KEY POINT:

> *It is envisaged that this timely analysis will provide readers with a legally informed understanding of sovereignty against which the legitimacy of activities – including activities undertaken by Australian actors – in cyberspace and space can be analysed, reducing potential for misunderstandings and conflict.*

[3] Department of Defence, *2016 Defence White Paper* (25 February 2016) <https://www.defence.gov.au/WhitePaper/Docs/2016-Defence-White-Paper.pdf> ('*2016 White Paper*').

The Report is set out as follows:

Chapter 1 – Introduction
Chapter 2 – The concept of sovereignty
Chapter 3 – The concept of sovereignty in the cyber domain
Chapter 4 – The relevance for Defence of the developing concept of sovereignty in the space domain
Chapter 5 – Concluding remarks

In this introductory chapter, we have considered recent literature pertinent to the debate to show why it is important for Defence and policy planners to understand the significance associated with understanding and considering sovereignty in a Defence context. Chapter 2 of the Report provides readers with a critical analysis of the concept of sovereignty, how it has developed and how the concept may be constructed, informed by recent and ongoing critical debate. Chapter 3 considers how the concept of sovereignty may apply in the emerging domain of cyberspace, while Chapter 4 considers sovereignty's application to the Space domain. Chapter 5 provides some concluding thoughts and recommendations for future consideration.

We encourage readers to read the complete Report but note that each chapter may be considered as a standalone document for members of an interest specific audience.

Why it matters: Defence policy on the space and cyber domains

Over the past half century, technological developments associated with both the digital revolution and the space race have fundamentally changed the world around us. Networked information and communication technologies, with their reliance on technologies including satellite relays, the Internet, and data digitisation are now integral to almost every aspect of human endeavour. These technologies are value neutral and dual purpose: they underpin the full array of military and civilian activities and functions; and can be exploited for purposes that are benevolent or malicious.

In addition to non-military uses, space and cyberspace have emerged as domains of relevance to military applications, alongside the traditional domains of land, sea, and air. Australia, consistent with the practice of other nations, has highlighted the strategic importance of space and cyberspace to Australia's national interests though high-profile defence and civilian investments in space and cyberspace capabilities.

Australian Defence policy published throughout the last two decades has increasingly sought to emphasise the challenging nature of protecting Australia's national interests in cyberspace and space.

The threat to national security posed by cyber-attacks on defence, government, and commercial communications networks was identified in the 2009 White Paper, followed by confirmation in 2011 that cyber activity falls within the scope of the ANZUS treaty.[4] In the 2013 White Paper, both Cyber and Space Situational Awareness and Mission Assurance were identified as Joint Enabling Forces, the inclusion of the former largely reflecting the restructuring and rebadging of the Defence Signals Directorate into the Australian Signals Directorate, announced shortly prior to the release of the 2013 White Paper. However, neither space nor cyber expressly appear in the list of threats the ADF must be

[4] Ibid, 123.

prepared to respond to identified in the 2013 White Paper.[5] Writing in 2015, Colonel Michael Lehmann supported the introduction of cyberwarfare as a capability in the 2009 Defence White Paper and argued that ADF thinking should turn to rapidly developing an offensive cyber capability.[6]

The 2016 Defence White Paper expressly identified 'intelligence, surveillance and reconnaissance, space, electronic warfare, and cybersecurity' as a stand-alone capability priority, on equal footing with maritime operations, strike and air combat, and land combat and amphibious forces, and identified 'complex, non-geographic threats including cyber threats' as a driver of Australia's national security environment out to 2035.[7]

Express inclusion of cybersecurity and space as components of a broader key capability in White Paper 2016 coincided with an overt Defence and security policy commitment to preservation of a stable rules-based global order:

> The Government is committed to making practical and effective military contributions to global security operations to maintain the rules-based order and address shared security challenges where it is in our interest to do so.[8]

The White Paper noted that the rules based global order 'supports the peaceful resolution of disputes, facilitates free and open trade and enables unfettered access to the global commons to support economic development'.[9] The paper goes on to state:

> Underpinning the rules-based global order is a broad architecture of international governance which has developed since the end of the Second World War. ... The framework of the rules-based global order is under increasing pressure and has shown signs of fragility. The balance of military and economic power between countries is changing and newly powerful countries want greater influence and to challenge some of the rules in the global architecture established some 70 years ago. While it is natural for newly powerful countries to seek greater influence, they also have a responsibility to act in a way that constructively contributes to global stability, security and prosperity. However, some countries and non-State actors have sought to challenge the rules that govern actions in the global commons of the high seas, cyberspace and space in unhelpful ways, leading to uncertainty and tension.[10]

The strategic guidance contained in the 2016 White Paper presents the space domain as an enabler, the electromagnetic spectrum a resource to be controlled and cyberspace as an environment (domain) that requires protection to allow national interests to operate without intrusion or disruption. It notes for example the influence of 'non-geographic threats, such as threats in cyberspace and space' in shaping the strategic environment.[11] Elsewhere, it identifies cyber-attacks as 'a direct threat to the ADF's warfighting capability' reflecting ADF dependence on networked information systems,[12] including space-based satellite systems which support 'networked capabilities', and the increased access to offensive cyber-operations capabilities of both State and non-State actors.[13] The White Paper noted the need for the international community

[5] *2016 White Paper* (n 3) 45.
[6] COL Michael Lehmann, 'The Case for an Offensive ADF Cyber Capability: beyond the Maginot mentality' (2015) 198 *Australian Defence Force Journal* 31.
[7] *2016 White Paper* (n 3) 40.
[8] Ibid 15.
[9] Ibid 44.
[10] Ibid 46.
[11] *2016 White Paper* (n 3) 16.
[12] Ibid 51.
[13] Ibid 52.

to work cooperatively to establish a rules-based system to govern the use of outer space – but also noted that such cooperation was unlikely to occur in the short term.[14] Instead, the government identified investment in 'Defence's space surveillance and situational awareness capabilities' in order to 'ensure the security of our space-based capabilities'.[15]

In 2017, an assessment of the importance of securing the space domain was presented by Air Commodore Chris Westwood in, 'Securing space: Australia's urgent security policy challenge for the 21st century'. Air Commodore Westward argued:

> While there has been very little effort in Australia to ensure that its space interests are secure, many other nations have acknowledged this vulnerability and are now investigating options to secure space. This is a very complex challenge. There is no global consensus regarding how to secure space, with various nations considering options such as treaties, codes of conduct and even weaponising space. This paper proposes a national-level policy to establish a foundation for securing Australia's future space activities.[16]

Another call for the Australian Defence Force to consider contested space came from Mr Malcolm Davis, writing for the Australian Strategic Policy Institute in 2019. Davis noted that current joint Australian Defence Force doctrine identified space (and arguably cyberspace) as a centre of gravity in information-based operations. Simply, Davis argued, 'the ADF can't use military power quickly, precisely and decisively without it. Space enables our forces to exploit an information edge to constrain the risks of high casualties in a prolonged conflict, while maximising our tactical edge and avoiding operational surprise'.[17]

Critically, Davis pointed out that:

> Space is a war-fighting domain and, while the ADF doesn't seek to weaponise space, it does seek to set the conditions to ensure its access to this critical environment. Although space is a global common—much like the oceans or cyberspace—it isn't a sanctuary that sits placid and serene, untouched by terrestrial geopolitical rivalry and conflict below.[18]

Combined, these examples of recent Defence-centric commentary establish that Defence has a good understanding of the threats and sought-after capabilities inherent to each domain. But, as Major General Marcus Thompson, then Head of the Army's Information Warfare Division, writing in 2016 observed, 'if the ADF is to fight and win in a hostile cyber environment, it must consider the types of cyber capabilities it needs – and how those capabilities might be developed and applied in order to achieve an advantage in the contemporary battlespace'.[19] Truly understanding how to fight either domain requires an understanding of the future of war which is an inherently human activity governed by legal frameworks.

In 'Predicting Future War', Dr Robert A. Johnson makes the point that Defence planners need to investigate the need to consider the characteristics of future war and the operating environment in which it may be fought. However, he also notes:

> ...legal frameworks for Western operations will become less flexible and military officers express a fear they will be too

[14] Ibid 53.
[15] Ibid 87.
[16] MAJ Christopher Wardrop, 'Bridging the gap between cyber strategy and operations: a missing layer of policy' (2014) 204 *Australian Defence Force Journal* 61.
[17] Malcom Davis, 'The Australian Defence Force and contested space' (Article, 15 August 2019) <https://www.aspi.org.au/report/australian-defence-force-and-contested-space>.
[18] Ibid.
[19] MAJGEN Marcus Thompson, 'The ADF and Cyber Warfare' (2016) 200 *Australian Defence Force Journal* 43.

> constrained to manoeuvre at all in the future. Legal advisors are vital in low-intensity operations among the people and in counterterrorism but would have less bearing on high-intensity campaigns. Indeed, it should be noted that legal advice in Western countries have tended to facilitate rather than obstruct operations. The real obstacle is risk-aversion and fear of 'juridification' of operations at the strategic and policy-making level. [20]

In support of his argument that Defence planners need to investigate and consider the characteristics of future war and the operating environment in which it may be fought, Johnson made the point that anxiety about Western vulnerabilities has led to speculative concerns about 'e-warfare, counter-terrorism scenarios, inter-robotic battles and the future of unmanned air power to conduct standoff attacks'.[21] Whilst debate will continue as to the characteristics of future war, the fact remains that in cyberspace and space, hostile acts are not the remit of nation States because the prevalence of modern information and communications technologies has resulted in individuals having access to resources and computing power that can affect a nation State's interests.

This 'nonconventional', 'hybrid' or 'grey zone' warfare is now considered part of a multidomain warfighting approach that adversaries can use to disrupt, degrade or disable an opponent's capabilities without ever engaging in open and attributable hostilities.[22] In 2019, Bachmann, Dowse and Gunneriusson extended the use of non-traditional capabilities to include 'law as a weapon' used to manipulate legal paradigms. They argue that Russia and China (in particular) have employed a form of weaponised law, or 'Lawfare', as a mode of hybrid warfare or as an element of influence operations.[23] Further, 'Lawfare', as practiced by those nations, 'provides a layer of 'fake' legitimacy, or at least reduces the erosion of apparent legitimacy, due to the nonattributable aspects inherent in hybrid warfare while using 'easy' hybrid warfare methods'.[24] Further, the authors also note that, 'General Campbell [Chief of ADF] pointed out that Australia and similar democratic nations need to better develop counters to political warfare threats such as disinformation, cyber, IP theft, coercion and propaganda. He also

KEY POINT:

Whilst debate will continue as to the characteristics of future war, the fact remains that in cyberspace and space, hostile acts are not the remit of nation States because the prevalence of modern information and communications technologies has resulted in individuals having access to resources and computing power that can affect a nation State's interests.

[20] Robert A. Johnson, 'Predicting Future War' (2015) 196 *Australian Defence Force Journal* 70.
[21] Ibid.
[22] Sascha Dominik Bachmann, Andrew Dowse and Hakan Gunneriusson, 'Competition short of war – how Russia's hybrid and grey-zone warfare are a blueprint for China's global power ambitions' (2019) 1(1) *Australian Journal of Defence and Strategic Studies* 41.
[23] Ibid 50 citing Sascha Dominik Bachmann and Andres Munoz Mosquera, 'Hybrid Warfare as Lawfare: Towards a Comprehensive Legal Approach A Civil-Military Response to Hybrid Threats' in Elsa Cusumano and Marian Corbe (eds) *A Civil-Military Response to Hybrid Threats* (Springer, 2017).
[24] Ibid.

highlighted the importance of countering grey-zone tactics in the shaping and influencing phases of conflict, rather than when events cross the threshold of war'.[25] This is instructive as it provides insight into the Chief of the Defence Force's thoughts and suggests that Defence is increasingly thinking of the cyberspace and space domains as integral to the strategic, operational and tactical battlespace.

To date, much Defence writing on space and cyberspace engages in effects-based capability analysis of the cyberspace and space domains. In contrast, comparatively little has considered how the concepts of sovereignty and jurisdiction proscribe the legitimacy or otherwise under the international legal system of engaging in activities within these domains.

To maintain consistency with the Australian Government's stated commitment to 'rules-based global order', it is necessary to critically examine the substance and effect of policy statements invoking sovereignty as a fundamental consideration of what constitutes legitimate actions. Without this understanding, statements like: 'Sovereignty delineates the scope of legitimate State activity, including in cyber and space environments, both identified as threats to the strategic environment',[26] from the 2016 Defence White Paper, lack context and substance.

Marigold Black, an Army Research Centre Research Fellow considering the 2016 White Paper noted the lack of consensus understanding of the meaning of sovereignty when used in the White Paper and Defence policy documents more broadly, observing:

> While references to sovereignty are not uncommon in Australia's national security and defence discourse, the term is typically employed without qualification or elucidation, even as the stakes could not be higher. There appears to be a lack of meaningful engagement among policymakers, analysts and commentators with the contours of Australia's national sovereignty, and with the importance of articulating those parameters for Defence strategy. The sovereignty concept recurs in debates concerning, for example, external interference in political institutions, the need for a sovereign Defence industry, and the protection of national borders; yet some of the most fundamental definitional questions are left unanswered.[27]

This gap may then lead to Defence planners being at risk of succumbing to what Kilcullen has termed 'conceptual envelopment'.[28] He uses the term to describe a:

> situation in which an adversary's conception of war becomes so much broader than our own that two dangerous things can happen. First, that adversary may be acting in ways it considers warlike, while we with our narrower notion of warfare remain blithely unaware of the fact, so that by the time we realise we are at war, we have already lost. Second, and what is even more dangerous, we can be taking actions that we define as normal peacetime competition, while a rival with a broader concept of conflict sees these as acts of war and responds accordingly. At worst, each of us may completely misunderstand the other's motivation, strategy, and outlook, risking lethal miscalculation.[29]

The conceptual basis of sovereignty becomes even less clear once one moves beyond the White Papers into other capability policy documents. The Defence Industrial Capability Plan for example

[25] Ibid.
[26] *2016 White Paper* (n 3) 51.
[27] Marigold Black, 'In defence of Australian Sovereignty' (Online, 12 June 2018) < https://researchcentre.army.gov.au/library/land-power-forum/defence-australian-sovereignty>.
[28] David Kilcullen, *The Dragons and the Snakes – How the Rest Learned to Fight the West* (Hurst, 2020).
[29] Ibid 175.

outlines the Sovereign Industrial Capability Assessment Framework, in order to identify Sovereign Industrial Capability Priorities. Rather than formulating a distinct definition of sovereignty, however, the concept is loosely defined as related to other, complex concepts including 'access and control over technology, essential skills, intellectual property, financial resources and infrastructure'.[30] Rather than providing a definition of sovereignty, therefore, the framework instead provides a laundry list of manifestations of concepts that may arguably be protected by or subject to sovereignty- quite a different undertaking.

Australia's need to formulate a coherent understanding of sovereignty in the context of the space and cyberspace domains becomes even more pressing in light of increasingly public ambitions to develop offensive cyberspace capabilities.

The 2020 Strategic Update, and the 2020 Force Structure Plan, further develop Australia's commitment to rules-based order and to developing space and cyberspace capabilities. The Strategic Update, released after the emergence of the COVID-19 pandemic, notes that the strategic environment deteriorated more rapidly than anticipated in the 2016 White Paper, requiring adjustment to the strategy outlined in the 2016 White Paper. Those adjustments include reconfiguring Defence capabilities to recognise information and cyber capabilities, and space capabilities, as stand-alone separate capability pillars, alongside maritime capabilities, air capabilities, and land capabilities. That consolidation of key capability status for both cyber and space reflects recognition of the role of cyber and space in many of the emerging and adapting strategic threats driving the 2020 Strategic Update. These threats include 'grey zone' activities - non-military coercive tactics deployed against States by other actors to challenge sovereignty and undermine traditional or established regional partnerships, potentially facilitated by cyber warfare or use of cyber platforms to spread disinformation; and expansion of malicious cyber capabilities by State and non-State actors, including through dissemination of disinformation, direct targeting of military activities, and compromise of critical infrastructure. The 2020 Strategic Update also expressly states that Defence will 'invest in offensive cyber and operational cyberspace capabilities for deployed forces'.[31] Providing more detail to the 2020 Strategic Update, the accompanying 2020 Force Structure Plan describes the required Joint Cyber capability requirement to be:

> able to exploit and attack adversary information networks, while protecting our own networks, mission systems and platforms across the tactical to strategic spectrum. This program provides the systems to enable Defence to conduct defensive and offensive cyber operations against a range of adversaries for military purposes, and to effectively counter cyber-attacks on Australia, on Defence, and on deployed forces.

Read in light of the broader reaching overarching strategic objectives stated in the 2020 Strategic Update- to deploy military power to shape Australia's strategic environment, deter actions against our interests and, when required, respond with credible military force - it becomes apparent that Defence requires greater clarity about the concept of sovereignty in order to distinguish between technologically feasible options which may differ significantly in legitimacy in the eyes of the international community.

[30] Department of Defence, 'Sovereign Industrial Capability Priorities', *Department of Defence* (Web Page) < https://www1.defence.gov.au/business-industry/capability-plans/sovereign-industrial-capability-priorities> accessed 30 May 2021.
[31] *2020 Defence Strategic Update* (n 1) 36.

As Black noted:

> To know and understand the parameters of Australian sovereignty is to lay the foundations for a serious argument about what is to be protected and why, and the means by which to secure and project Australian power in an increasingly hostile, and uncertain world.[32]

It is the aim of this project to facilitate understanding of those parameters, and to lay those foundations.

[32] Black (n 27).

CHAPTER

2

The concept of sovereignty

CHAPTER 1: The concept of sovereignty

The concept of sovereignty 12
- Sovereignty in the defence context 12
- Sovereignty in legal theory 14
- Sovereignty in international law 14
- Sovereignty in international relations 16

Conceptual issues and debates 17
- Sovereignty as inherent or contested 17
- Sovereignty as right, privilege, power or immunity 18
- Sovereignty as a rule or a principle 18

Refining the concept of sovereignty 19
- Sovereignty as a practice 19
- Sovereignty as a functional concept 19
- Sovereignty as a bundle concept 20

Implications for the defence context 21
- Sovereignty and defence coordination 21
- A pragmatic pluralist framework 22

The concept of sovereignty

The concept of sovereignty has evolved over time in both international law and international relations. In general, it concerns States exercising authority over matters within their jurisdiction. Sovereignty is both constitutive of international law--in the sense that international legal norms were traditionally predicated on the sovereignty of States and their consent to be bound — and impacted by it. Human rights norms, for example, may affect a State's sovereignty without its consent.

Sovereignty is negotiable in the sense that States may decide to waive, on a temporal or ongoing basis, aspects of their sovereignty by consenting to be bound by norms of conduct with respect to other States. It has been suggested that sovereignty is a commodity that can be traded by a State to its advantage.[33] The commodity model of sovereignty assumes a baseline allocation of jurisdiction to each State that can then be traded. However, perhaps unsurprisingly given its strategic importance, the content of this baseline allocation itself continues to be disputed.

Sovereignty in the defence context

Sovereignty has a particular resonance in the defence context. Traditionally, as already noted, State sovereignty has been linked to security and the capacity to make war.[34] Historically, States had a sovereign privilege to wage war,

[33] Georg Nolte, 'Sovereignty as Responsibility' (2005) 99 *Proceedings of the Annual Meeting (American Society of International Law)* 389.
[34] Janice E Thomson, 'State Sovereignty in International Relations: Bridging the Gap between Theory and Empirical Research' (1995) 39(2) *International Studies Quarterly* 213, 213.

whereas now international law prohibits the use of force unless other than under the UN Charter. This reflects the presumed legitimacy of a State's military capacity and its ability to defend its national interests.

One view sees the defensive aspect of sovereignty as a way of serving global political, economic and security needs.[35] It is a way of dividing capacities and ensuring stability in the global order. Another (realist) view sees it as reflecting power-seeking by States. States insist on sovereignty as they seek to build influence in competition with other States or, for the less powerful, to defend themselves against inevitable predation by other entities.

States are juridically equal under international law but unequal in defensive capabilities and strategic influence. There is a disjunction between the purported egalitarianism of international law and the political realities of international relations. This tension manifests itself in the defence context through the universal application of humanitarian law, on the one hand, and the reality of selective observance and enforcement, on the other.[36]

Sovereignty in the defence context is tied to a State's defensive capabilities. States commonly justify investment in defensive capabilities as linked to securing national interests and thus maintaining sovereignty. This reflects the realist perspective discussed above. Sovereignty has been defined in the Australian national defence context as 'the ability to independently employ defence capability or force, when and where required ... with or without our allies'.[37]

Defensive sovereignty is also often linked to the concept of self-reliance in national security. Australia defence strategy involves a focus on small and medium enterprises to develop technologies needed to maintain defensive capabilities.[38] Sovereignty in the defensive sense is also often defined to include management of cross-border flows of people and goods, reflecting the traditional focus on territorial integrity.[39]

Defensive sovereignty is subject to political realities. Few States are entirely militarily self-reliant and most do not aspire to be so. Frühling suggests that 'arguably only the major nuclear powers (US, Russia and China) ... can be said to be truly sovereign, in that they control all the resources required for their own defence'.[40] This conception of defensive sovereignty is

[35] Ibid, 216.
[36] Jonathan Crowe, 'Coherence and Acceptance in International Law: Can Humanitarianism and Human Rights be Reconciled?' (2014) 35 *Adelaide Law Review* 251.
[37] Brendan Nicholson, 'A Sovereign Defence Industry for Australia', *The Strategist - Australian Strategic Policy Institute* (Article, 24 April 2018) <https://www.aspistrategist.org.au/sovereign-defence-industry-australia/>.
[38] Stephan Frühling, 'Sovereign Defence Industry Capabilities, Independent Operations and the Future of Australian Defence Strategy' [2017] (October) *The Centre of Gravity Series, Australian National University*, 2, 2.
[39] Ibid, 3.
[40] Stephan Frühling, 'Sovereign Defence Industry Capabilities, Independent Operations and the Future of Australian Defence Strategy' [2017] (October) *The Centre of Gravity Series, Australian National University*, 4.

unrealistic, unnecessary and probably undesirable for most nations.

Sovereignty in legal theory

Early international law scholars developed a relatively unsubtle but influential analysis of sovereignty as ultimate power within a jurisdiction.[41] The traditional notion of sovereignty concentrates power within the hands of a single actor within the territory. This aspect was emphasised by Bodin, Hobbes and Vattel.[42] The traditional view also emphasised the sovereign equality of States. This is found particularly in the work of Grotius.[43]

Sovereignty, even on the traditional model, is not truly unlimited. The concept of sovereignty includes at least three inherent limitations.[44] First, it is subject to jurisdictional limits: a sovereign body cannot act outside its authority. Second, sovereignty is subject to practical limits: a sovereign body may face difficulties imposing a measure it lacks the power to enforce. Third, sovereignty is subject to normative limits. Grotius, for example, argued that all sovereign States are subject to the mutually accepted rules of the international order.[45]

Each of these limitations plays a role in sovereignty in the international sphere. International sovereignty is inherently tied up with questions of jurisdiction. This can be seen in the dispute over baseline allocation described above. International sovereignty also implicates questions of power, since in practical terms, a State's sovereignty is impacted by what it has effective power to do. Finally, international sovereignty has expanded normative limits, due to the growth of human rights standards in international law.

Sovereignty in international law

Sovereign States continue to be the primary subjects of binding international law norms.[46] State sovereignty under international law has both an internal and an external aspect.[47] The internal aspect concerns the State's ability to control what occurs within its territory without interference. The external aspect concerns the State's capacity to control its relations with other States, including what rules and institutions bind it. However, both forms of sovereignty are determined and limited by jus cogens norms and customary law more broadly.

Traditional views of State sovereignty, as discussed previously, assumed absolute authority within defined territory.[48] However, developments since World War II have undermined this conception. These include the

[41] Ivan Simonovic, 'Relative Sovereignty of the Twenty First Century' (2002) 25 *Hastings International & Comparative Law Review* 371, 377.
[42] Joan Fitzpatrick, 'Sovereignty, Territoriality, and the Rule of Law' (2002) 25(3) *Hastings International and Comparative Law Review* 303 ('*Fitzpatrick*'), 308; Stephen D Krasner, 'Abiding Sovereignty' (2001) 22(3) *International Political Science Review* 229, 232.
[43] Mark Weston Janis, 'Sovereignty and International Law: Hobbes and Grotius' in T'ieh-ya Wang and Ronald St J Macdonald (eds), *Essays in Honour of Wang Tieya* (M Nijhoff Publishers, 1994) 391, 396-7 ('*Janis*').
[44] Jonathan Crowe, *Australian Constitutional Law: Principles in Movement* (Oxford University Press, 2022), ch 12 (forthcoming).
[45] Janis (n 43) 397.
[46] Samantha Besson, 'Sovereignty, International Law and Democracy' (2011) 22(2) *European Journal of International Law* 373, 376 ('*Besson*').
[47] Gary P Corn and Robert Taylor, 'Sovereignty in the Age of Cyber' (2017) 111 *AJIL Unbound* 207, 209 ('*Corn and Taylor*').
[48] Besson (n 46) 373.

growth of supranational organisations and NGOs, as well as globalisation and the emergence of international human rights.[49] These trends have led to increased recognition of sovereignty's practical and normative limits.

The traditional view of sovereignty was closely linked to territory.[50] The corollary of territorial sovereignty is the principle of non-intervention whereby States will not interfere in each other's internal affairs.[51] Traditional views of sovereignty are also linked to the legitimacy of independent military power.[52] A sovereign State is entitled to maintain the military means of protecting its independence if needed.

However, the territorial conception of sovereignty is challenged by recent developments. These include threats to sovereignty, such as global terrorism and cyber-attacks, which do not follow territorial boundaries.[53] States can no longer preserve their internal sovereignty solely or even primarily by policing their geographical borders. The precise content of sovereignty is constantly being renegotiated. State sovereignty, in this respect, is more accurately viewed as a 'legal construct' rather than reflecting fixed and unchanging entitlements of States.[54] It allocates recognised capacities among States that can then be limited or traded off among them by mutual consent. State sovereignty is therefore both a source of international law and a consequence of it.[55]

Sovereignty under international law belongs to all States.[56] This reflects the traditional conception of sovereign equality, as mentioned above. The extent to which sovereignty is respected, however, may depend on the power of the State concerned.[57] Goldsmith argues '[t]here has always been an enormous gap between norms of sovereignty and the behavior of nations.'[58] Krasner speaks of the 'organised hypocrisy' whereby States who benefit from recognition of sovereign norms will violate those norms in the national interest.[59]

---

[49] Jack Goldsmith, 'Sovereignty, International Relations Theory, and International Law' (2000) 52(4) *Stanford Law Review* 959, 959 ('*Goldsmith*'); Seyla Benhabib, 'Carl Schmitt's Critique of Kant: Sovereignty and International Law' (2012) 40(6) *Political Theory* 688, 701.
[50] Fitzpatrick (n 42) 307.
[51] Andreas Osiander, 'Sovereignty, International Relations, and the Westphalian Myth' (2001) 55(2) *International Organization* 251, 266.
[52] Ibid, 277.
[53] Fitzpatrick (n 42) 308.
[54] Besson (n 46) 380.
[55] Ibid, 385.
[56] UN Charter, art 2(1).
[57] Bardo Fassbender, 'Sovereignty and Constitutionalism in International Law' in Neil Walker (ed), *Sovereignty in Transition* (Hart, 2014), 120-1 ('*Fassbender*').
[58] Goldsmith (n 18) 960.
[59] Stephen D Krasner, 'Abiding Sovereignty' (2001) 22(3) *International Political Science Review* 229.

Sovereignty as a legal concept can be seen as legitimating power and authority within the international system.[60] It is an 'institutional fact', meaning it guides State behaviour and is shaped by how States interact with it.[61] Sovereignty confers on States the status needed to legitimate certain rights, duties and competencies.[62] Mutual recognition among States of the features of sovereignty is required for it to play its normative role.

Sovereignty in international relations

Sovereignty in international relations can be viewed as a way of dividing up power among States to ensure a workable system. It 'defines the terms of legitimate statehood.'[63] Baylis et al argue that the international system relies on a dichotomy between the realm inside the sovereign State, which is viewed as stable and orderly, and the international sphere, which is anarchical.[64] The reality is, of course, more complicated.

Sovereignty provides order to the international space by dividing spheres of authority and allowing States to police them. This division of power is maintained by the traditional picture of sovereignty as a 'fixed and exogenous' attribute of States.[65] This traditional conception masks the reality that sovereignty is political and subject to negotiation. It is a socially constructed concept produced through practice and redefined over time.[66]

Sovereignty as a practical concept in international relations also reflects hierarchies. The elements of hierarchy in the international system — produced by wealth, resources and strategic positioning — influence both how sovereignty is understood and the extent to which it is respected. Sovereignty and hierarchy in the international system are relational, as they depend on diplomatic and trading alliances, as well as supranational organisations.[67]

Krasner influentially argues that international sovereignty, while traditionally portrayed as sacrosanct, is actually frail.[68] There are numerous examples in history of States interfering with each other's territory and citizens. Sovereignty in international relations is the subject of negotiation among rulers and heads of government, who are primarily guided by domestic

---

[60] Wouter G Werner and Jaap H De Wilde, 'The Endurance of Sovereignty' (2001) 7(3) *European Journal of International Relations* 283, 290 ('*Werner and Wilde*').
[61] Ibid, 291-2.
[62] Ibid, 297.
[63] John Baylis and Steve Smith and Patricia Owens, *The Globalization of World Politics: An Introduction to International Relations* (Oxford University Press, 5th ed, 2011), 280.
[64] Ibid, 174.
[65] David A Lake, 'The New Sovereignty in International Relations' (2003) 5(3) *International Studies Review* 303, 305.
[66] Ibid 307.
[67] Ibid 313-14.
[68] Stephen D Krasner, *Sovereignty: Organised Hypocrisy* (Princeton University Press, 1999).

constituencies and not international legal norms.[69]

Traditional sovereignty on the international level only attaches to nation States. Views differ in the international relations literature on whether this is still the case.[70] Some authors argue that States are no longer the only repositories of sovereignty in the international system, given the international personhood of individuals and groups under human rights law, along with the rise of supranational organisations. Others contend that the primacy of State sovereignty endures and underpins these ostensible new forms of authority.

Krasner develops a model of 'shared sovereignty' involving voluntary agreements between recognised political authorities and external actors.[71] This model presents a policy option for States to follow in negotiating the globalised international landscape. However, the model is premised on the traditional view of State sovereignty, insofar as it requires States to agree to share their authority with others. Krasner sees it as a settlement driven by domestic and global politics rather than reflecting a shift in sovereignty itself.[72]

Conceptual issues and debates

The preceding discussion of the concept of sovereignty reveals some underlying conceptual issues and debates. We discuss three of these before proceeding to refine the concept. The first relates to whether sovereignty is an inherent attribute of States or necessarily contested. The second concerns whether sovereignty is best viewed as a right, privilege, power or immunity. The third concerns whether sovereignty is a rule or a principle.

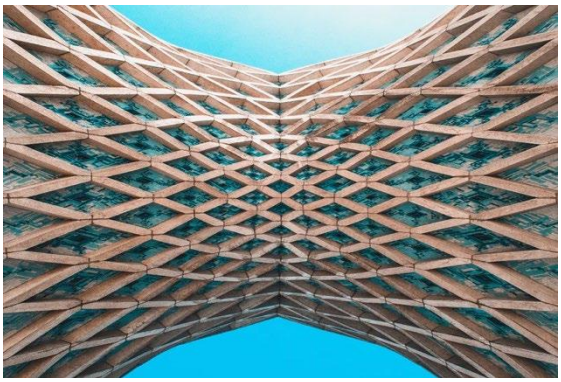
Sovereignty as inherent or contested

Traditionally sovereignty has been treated as an inherent attribute of States.[73] All States are sovereign by virtue of their statehood. The notion of sovereign equality is a fundamental principle of the United Nations.[74] This suggests that States, by their nature, have certain inherent entitlements. Classical theories of sovereignty supported this notion by recourse to natural law like reasoning,[75] often with a theistic dimension.[76]

The inherent view of State sovereignty has come under sustained criticism from realist authors.[77] These authors have pointed out that the precise boundaries of sovereignty are contested and reflect global power structures. The traditional model serves to mask

[69] Ibid.
[70] Jens Bartelson, 'The Concept of Sovereignty Revisited' (2006) 17(2) *European Journal of International Law* 463, 464-5.
[71] Stephen D Krasner, 'The Case for Shared Sovereignty' (2005) 16(1) *Journal of Democracy* 69, 70.
[72] Ibid, 71-3.
[73] David A Lake, 'The New Sovereignty in International Relations' (2003) 5(3) *International Studies Review* 303, 305 (*'Lake'*).
[74] UN Charter, art 2(1).
[75] Fassbender (n 57) 121.
[76] Jacques Maritain, 'The Concept of Sovereignty' (1950) 44(2) *The American Political Science Review* 343, 344-7.
[77] Lake (n 73) 307.

the realities of international relations and, in particular, the hierarchies of the international system. It therefore misses an important dimension of the concept of sovereignty.



The realist view does not mean sovereignty lacks stable content. Sovereignty can be viewed as a socially constructed practice with some core features, while also being subject to modification over time. This approach avoids the unrealism of the traditional view, recognising political realities. However, it also recognises a stable core to the notion of sovereignty, rather than abandoning the attempt to conceptualise it entirely.

Sovereignty as right, privilege, power or immunity

Sovereignty has been variously depicted as a right, privilege, power or immunity of States. These terms are used in various ways, but they are clarified by the influential work of W N Hohfeld.[78] Hohfeld defined a right (in the strict sense) as a claim that someone else do or not do something; it correlates to the other person's duty. A privilege, for Hohfeld, is the liberty to do or not do something, unfettered by anyone else's right.

A power, according to Hohfeld, is the ability to change someone else's legal position by acting in a certain way. A person's immunity, on the other hand, means that another person is unable to exercise a power with respect to them. Hohfeld's analysis is useful for delineating legal relationships in a fine-grained way. He observes that the term 'right' is often loosely used to describe all the different concepts set out above.

State sovereignty can be viewed as containing aspects of right, privilege, power and immunity. A sovereign State has the right that other States not violate its territorial integrity. It has the privilege to govern its citizens as it wishes, subject to human rights. It has the power to enact domestic laws and enter into treaties. It has an immunity against other States imposing limits without its consent, subject again to fundamental norms.

Sovereignty as a rule or a principle

Is sovereignty a rule or a principle? The distinction between these concepts is often traced to the work of Ronald Dworkin.[79] A rule, for Dworkin, is an all or nothing standard. It rules out certain actions and permits others. A principle, by contrast, has what Dworkin terms 'a dimension of weight'.[80] It does not definitively rule out any given action, but rather counts in favour or against it, along with other relevant factors.

[78] Wesley Newcomb Hohfeld, 'Some Fundamental Legal Conceptions as Applied in Judicial Reasoning' (1913) 23 *Yale Law Journal* 16; Wesley Newcomb Hohfeld, 'Fundamental Legal Conceptions as Applied in Judicial Reasoning' (1917) 26 *Yale Law Journal* 710. For an overview, see Jonathan Crowe, *Legal Theory* (Thomson Reuters, 3rd ed, 2019), ch 8.
[79] For an overview, see Crowe (n 78) 177-85.
[80] Ronald Dworkin, *Taking Rights Seriously* (Harvard University Press, 1978), 26.

Some aspects of State sovereignty appear to have a rule-like character, due to the relatively clear-cut nature of the boundaries and low thresholds for violation. Territorial integrity is the obvious example. Traditionally, any incursion over a State's territorial borders by actors of another State is a violation of sovereignty.

However, sovereignty often seems to function more like a principle. It serves as a starting point for negotiations between States. It is negotiable, in the sense that States may be willing to trade off claims of sovereignty for economic or strategic advantage. We suggest below that both these concepts should be accommodated within a nuanced conception of sovereignty. Sovereignty has both rule-like and principle-like dimensions.

Refining the concept of sovereignty

This section develops a refined conception of sovereignty that incorporates the insights assembled above. It helps resolve the debates outlined in the previous section by synthesising the opposing viewpoints. The resulting view of sovereignty is pragmatic and realistic, making it well adapted for the defence context. It is suitable to respond dynamically to the challenges and opportunities posed by cyberspace and outer space jurisdiction.

Sovereignty as a practice

There is broad scholarly consensus that sovereignty is not static, but rather evolves over time. This reflects its political character. We suggest sovereignty is best understood as a socially constructed practice — although, as we clarify below, this does not mean it is devoid of stable content.

A practice in this sense is a set of normative standards developed over time by evolving consensus among members of a community.

The norms of sovereignty, on this view, emerge from the practices of nation States in their dealings with other international entities. There are, we suggest, elements of the practice that remain relatively fixed, such as a strong presumption of territorial integrity and the concept of sovereign equality. These elements represent the baseline allocation of entitlements among States that can then be traded off for other advantages.

Sovereignty as a practice can usefully be seen as containing what Hart famously called a core and a penumbra.[81] The core of the practice remains relatively unchanged over time. However, the penumbra is in a state of flux and is therefore more susceptible to variation. Cyberspace and outer space jurisdiction are currently penumbral areas of sovereignty, which partially explains their strategic importance in global politics.

Sovereignty as a functional concept

Practices often reflect human efforts to achieve shared goals. A practice is, in

[81] H L A Hart, 'Positivism and the Separation of Law and Morals' (1958) 71 *Harvard Law Review* 593, 607. For an overview, see Crowe (n 78) 173-4.

this sense, a teleological (or goal-oriented) notion.[82] Sovereignty, understood as a practice, can therefore be viewed as a functional concept.[83] Its precise attributes may be in a state of flux, but it can be analysed in terms of its purpose. This purpose brings a unity to the concept and helps us to understand its various components.

The function of sovereignty is plausibly to coordinate the interests of nation States in order to preserve global peace and security. It divides up territory and power between States in such a way as to avoid constant war and other forms of conflict. This is the baseline allocation of entitlements referenced previously. This conception of sovereignty's function is consistent with the fundamental aspirations of the United Nations.[84]

The traditional view of State sovereignty, often traced to the Peace of Westphalia, can be seen as serving this function. This view has been widely criticised as unrealistic in the contemporary context. However, it is possible to adopt these criticisms in a nuanced way without abandoning a functional view of sovereignty. Negotiations between States over sovereignty are attempts to maintain the peace by seeking a workable settlement.

Sovereignty as a bundle concept

Sovereignty, as discussed previously, is not a pure right, privilege, power or immunity. However, it contains each of these features within it. We suggest that, just as sovereignty has both an internal and external aspect, so too can it be analysed in terms of different legal relations between nation States and other entities. States have various rights, privileges, powers and immunities with respect to each other by virtue of their statehood.

Some incidents of sovereignty are relatively stable (like the right to territorial integrity) and others are more uncertain and contested. Another way of putting this is that some of the incidents of sovereignty are more rule-like whereas others function more like principles. The rule-principle distinction discussed previously is best seen as a continuum that helps capture the relative strength of sovereignty's various dimensions.

Werner and De Wilde argue that '[s]overeignty is not merely a bundle of

[82] Alasdair MacIntyre, *After Virtue: A Study in Moral Theory* (University of Notre Dame Press, 3rd ed, 2007), 187.
[83] For discussion, see Jonathan Crowe, *Natural Law and the Nature of Law* (Cambridge University Press, 2019), ch 9; Jonathan Crowe, 'Functions, Context and Constitutional Values' in Rosalind Dixon (ed.), *Australian Constitutional Values* (Hart, 2018).
[84] UN Charter, preamble, art 1.

rights, but consists in a status (being sovereign) and in the use of this status to legitimize certain rights, duties and competences'.[85] This observation is captured in our theory by the idea that States possess the incidents of sovereignty by virtue of their statehood. Statehood entitles States to the core presumptions of sovereignty such as territorial integrity and sovereign equality. It also gives them standing to negotiate over penumbral aspects.

Implications for the defence context

The conception of sovereignty developed above has important implications for the defence context. Sovereignty, on this view, is practice-based; it is functional; and it is essentially fungible. These features all make strategic positioning essential. They suggest a pragmatic but principled approach to sovereignty will best serve Australia's strategic interests in contested areas like cyberspace and outer space jurisdiction.

Sovereignty and defence coordination

The practice-based nature of sovereignty reveals that its real content comes from consensus in the international community. Legal rules, as discussed above, may set the framework for this consensus by outlining baseline allocations. However, the bulk of its content is negotiable. These negotiations do not occur in a vacuum, but against shared understandings of international actors about relevant rules and principles of sovereignty.

Australia's strategic interests are best advanced in this context through a coordinated approach to sovereignty that seeks interest-based alliances with other actors, including both States and other international organisations. Australia needs to forge consensus at the margins in order to influence sovereignty's emerging dimensions. A critical mass of support is ultimately needed to ensure any stable outcome from this process.

The functional nature of sovereignty is relevant here because it means States have a common interest in settled understandings on contested issues. A small number of powerful States may benefit in the short run from unsettling global normative consensus. This explains actions of the US, Russia and China in recent times. However, most States rely on a consensus to maintain international peace and security.

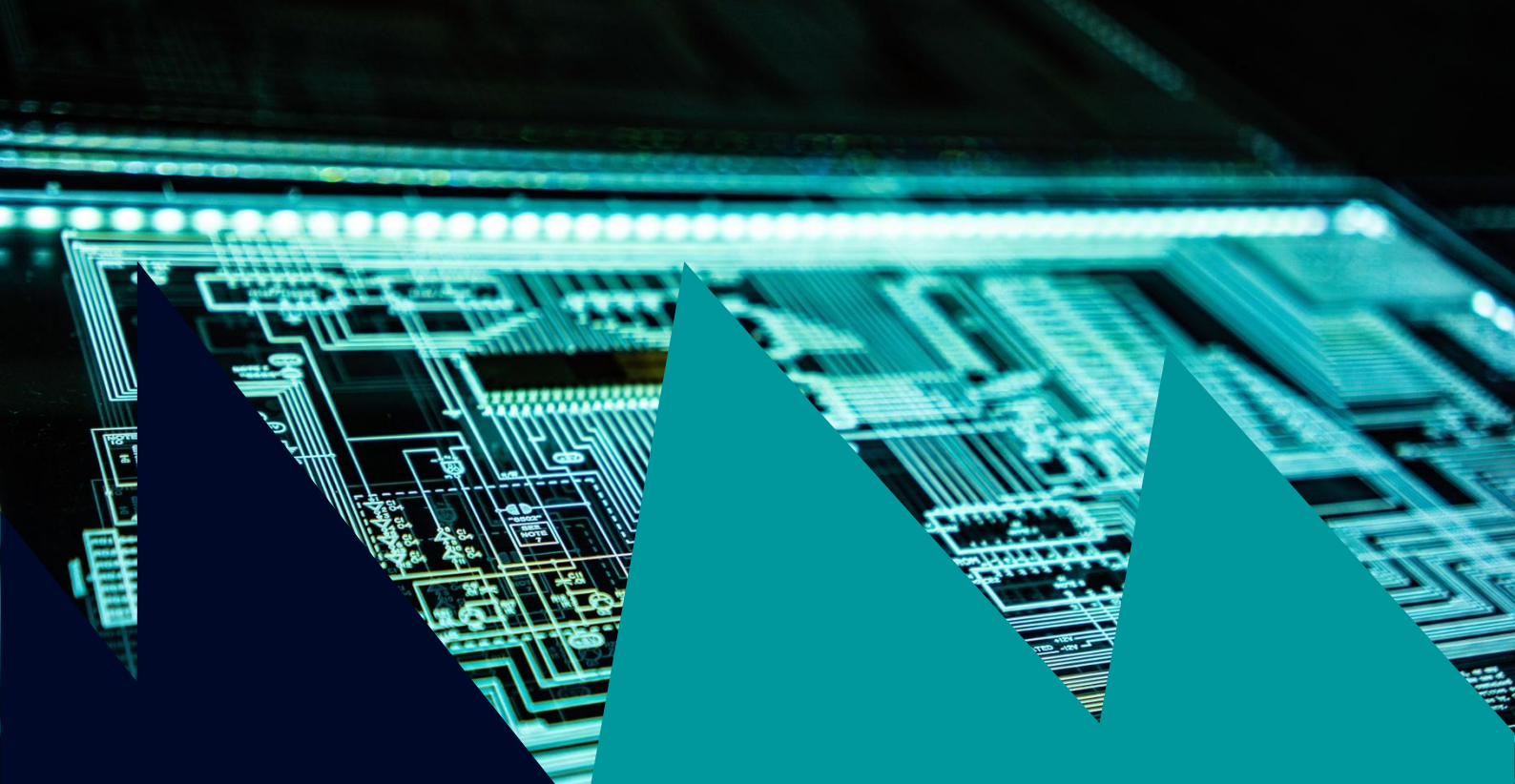
Australia can position itself as a forger of consensus on cyberspace and outer space sovereignty, thereby supporting the functional needs of most States while pursuing strategic settlements on the unsettled aspects of these concepts. This process should form part of Australia's broader strategy of defensive coordination. Local or targeted alliances can support this process while building towards consensus on a global level.

[85] Werner and Wilde (n 60) 297.

A pragmatic pluralist framework

Australia will be served by a pragmatic but principled approach to sovereignty in contested areas. Sovereignty, as described above, is relational. It comprises a bundle of relations between States and other entities. This has the consequence that sovereignty is pluralistic, at least at the margins. A State may advance different understandings of sovereignty depending on who it is dealing with. This will reflect the power dynamics and interests at play.

There is therefore room for pragmatism in seeking strategic alliances. However, Australia will also be served by maintaining a relatively principled and consistent view of sovereignty in its outward dealings. This is because the aim should be to forge a relatively stable consensus on the key aspects of sovereignty that serve Australia's interests. Consistency is needed on the relevant conception of sovereignty if this is to be achieved.



CHAPTER

3

The concept of sovereignty in the cyber domain

CHAPTER 2: The concept of sovereignty in the cyber domain

Background **24**
Internet governance and regulation 24
United Nations processes and international law 25
Sovereignty in cyberspace **27**
Overview of the debate 27
The current position of States on sovereignty 30
The non-intervention principle 33
The prohibition on the use of force 36
Examples of specific activities:
Disinformation operations 38
Cyber espionage 41
Cyber-attacks 42

New and emerging concepts of sovereignty 43

Concluding remarks regarding sovereignty in the cyberspace context 45

Background

Internet governance and regulation

The relationship between cyberspace and sovereignty was a central issue in the early Internet governance literature that began to emerge in the 1990s. One of the core questions in this literature was whether or to what extent sovereignty applied in cyberspace – that is, whether territorially based laws derived from sovereign States applied in the cyber context as in all other contexts, or whether new laws were needed given the unique characteristics of cyberspace (which placed this conceptual 'space' outside the sovereignty of States).[86] In a sense, the debate was centred around whether borders could be erected around the Internet making it a distinct domain outside the normal operation of State laws, or whether to extend some form of State-derived border onto the Internet.[87]

These debates, however, focused on sovereignty mainly in relation to Internet regulation, and the authority and ability of States to regulate activities by individuals and private entities online. While some of these issues continue in current debates about the governance of the Internet,[88] they are largely distinct from the current debate about the extent to which existing public international law (including on sovereignty) applies to State conduct in the cyber context. Put simply, it is now clear that law applies online and the ongoing matters debated relate to (1) what laws apply, and (2) who decides how those laws apply.

[86] See John P Barlow, 'Declaration of the Independence of Cyberspace', *Electronic Frontier Foundation* (Web Page, 8 February 1996) <https://www.eff.org/cyberspace-independence> accessed 18 November 2020; David Johnson and David Post, 'Law and Borders: The Rise of Law in Cyberspace' (1996) 48 *Stanford Law Review* 1367; Frank H Easterbrook, 'Cyberspace and the Law of the Horse' [1996] *University of Chicago Legal Forum* 207.
[87] See further: Dan Svantesson, 'Borders On, or Border Around – The Future of the Internet' (2006) 16(2) *Albany Law Journal of Science & Technology* 343 – 381.
[88] De La Chapelle, B. and L. Porciuncula (2021). We Need to Talk About Data: Framing the Debate Around Free Flow of Data and Data Sovereignty. Internet and Jurisdiction Policy Network.

KEY POINT:

...it is now clear that law applies online and the ongoing matters debated relate to (1) what laws apply, and (2) who decides how those laws apply.

United Nations processes and international law

At the United Nations (UN) level, States have agreed on the general application of international law to their activities in cyberspace. In 2013, a report from the UN Group of Governmental Experts (UN GGE) confirmed the general application of international law and UN Charter principles in relation to the ICT activities of States.[89]

This Report provided that:

> State sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities, and to their jurisdiction over ICT infrastructure within their territory.[90]

Subsequently, the 2015 report from the UN GGE also discussed sovereignty in connection with how international law applies to the use of ICTs by States:

> In considering the application of international law to State use of ICTs, the Group identified as of central importance the commitments of States to the following principles of the Charter and other international law: sovereign equality; the settlement of international disputes by peaceful means in such a manner that international peace and security and justice are not endangered; refraining 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; respect for human rights and fundamental freedoms; and non-intervention in the internal affairs of other States.[91]

Further, it provided that:

> In their use of ICTs, States must observe, among other principles of international law, State sovereignty, sovereign equality, the settlement of disputes by peaceful means and non-intervention in the internal affairs of other States. Existing obligations under international law are applicable to State use of ICTs. States must comply with their obligations under international law to respect and protect human rights and fundamental freedoms.[92]

In March 2021, the UN Open Ended Working Group (UN OEWG) on developments in the field of information and telecommunications in the context of international security released a consensus report in which UN Member States

[89] United Nations (UN) Group of Government Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN Doc A/68/98 (24 June 2013) 2.
[90] Ibid, 8.
[91] UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* UN Doc A/70/174 (22 July 2015) 12 ('*UN GGE Report 2015*').
[92] Ibid.

reaffirmed the application of international law to their use of ICTs.[93]

Essentially, while the UN GGE and UN OEWG have confirmed the general application of international law and identified the importance of State sovereignty, sovereign equality, the prohibition on the use of force, and the non-intervention principle, these reports have not provided detailed guidance on the specific ways in which these principles apply in the cyber context. For example, these reports do not provide clarity on (1) whether and when a cyber operation violates sovereignty: (2) when a cyber-attack constitutes a use of force; and (3) whether and when disinformation operations violate the non-intervention principle. Similarly, while the UN GGE and UN OEWG reports reflect the consensus of the States involved in these processes, they are not legally binding.

Generally, for international law to develop, States need to consent to new rules of law, for example, through treaties. But it can also develop through customary law which requires general practice by States, and that States undertake or engage in the practice out of a sense of legal obligation.[94] In the cyber context, this means that States could either agree to legally binding instrument (such as a treaty) detailing the rules and principles that govern their ICT activities or articulate the way in which they consider existing rules of law to apply in this context. Many States have begun doing the latter by expressing their official views on how they consider the law to apply. Importantly, States officially articulating their positions on matters such as sovereignty in cyberspace can help develop shared understandings and potentially lead to the development of customary international law.

In relation to the current debate about sovereignty in the cyber context, at this stage there is some divergence in views about the specific ways in which sovereignty (and other related rules or principles of international law) apply. This means that there continues to be uncertainty in the law and the precise way in which it applies is still evolving. This 'grey area' or 'grey zone' of the law – where there is a lack of clarity about how existing law applied and whether certain cyber activities are prohibited by these rules – provides States with a degree of freedom in their cyber activities. However, when conducting such activities, there is also a risk of escalation, particularly given the differences in understandings about whether and when cyber activities are in violation of international law. Further, a State's response to such activities may not

[93] UN Open Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, 'Final Substantive Report' *UN Office of Disarmament Affairs* (Online, 10 March 2021) 5-6 <https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf>.
[94] See UNGA Res 73/203, UN Doc A/RES/73/203 (20 December 2018).

be confined to the cyber context but can involve other diplomatic, economic, or kinetic measures.

In addition to the official views expressed by States about how the law applies in the cyber context, there is also extensive academic literature on this topic. While the views of academics and international law experts are not binding under public international law, they can and have influenced the views of States that have developed their legal positions on these issues. The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations ('Tallinn Manual')[95] which seeks to detail how international law applies in the cyber context (through a set of rules) along with detailed commentary to the rules has been particularly important in this context. While the Tallinn Manual is influential in this area and its drafting involved some consultation with States,[96] it is important to note that it is not a legally binding instrument. Further, its NATO origins means that it is far from universally accepted on the global arena.

Sovereignty in cyberspace

Overview of the debate

Sovereignty generally involves interrelated rights and correlating duties of States in relation to their territorial sovereignty; independence, and sovereign equality.[97] This means that States have the right to exercise jurisdiction within their territory; the freedom to conduct their own affairs independently; and (formal) equality of States under international law.[98] In the cyber context, it is generally accepted that States have sovereignty over the cyber infrastructure within their territory, as well as the cyber activities of individuals, groups, and organisations within their territory.[99] In other words, States can regulate the use of the ICT infrastructure

[95] Michael Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2nd ed, 2017) ('*Tallinn Manual*').

[96] The Tallinn Manual was written by a group of experts with the aim of providing guidance and clarity for States on how international law applies in cyberspace. The first version of the Tallinn Manual was published in 2013 focused on international law on the use of force and international humanitarian law. A second and more comprehensive version was published in 2017 which considered these and various other areas of international law as they intersect with cyberspace, including, for example, the law of the sea and outer space law. The drafting of the second version involved the so called 'Hague Process' in which State representatives from fifty countries were able to offer their input into the contents of the rules. See Michael Schmitt, 'Tallinn Manual 2.0 on the International Law of Cyber Operations: What It Is and Isn't', *Just Security* (Blog Post, 9 February 2017) <https://www.justsecurity.org/37559/tallinn-manual-2-0-international-law-cyber-operations>. See also Dan Efrony and Yuval Shany, 'A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice' (2018) 112 *American Journal of International Law* 583.

[97] Harriet Moynihan, 'The Application of International Law to State Cyberattacks Sovereignty and Non-intervention' (Chatham House Research Paper, 2019) 11 <https://www.chathamhouse.org/2019/12/application-international-law-state-cyberattacks>.

[98] Ibid 12-3.

[99] For example, according to the Tallinn Manual experts, all States 'enjoy sovereignty over any cyber infrastructure located on their territory and activities associated with that cyber infrastructure'. This encompasses the physical, logical and social layers of cyberspace – that is, the physical infrastructure (hardware, cables, routers, servers, computers, and so on), the connections between network devices (applications, data, protocols, and so on), and the individuals and groups engaged in cyber activities. States also have both 'internal' and 'external' sovereignty. Internal sovereignty refers to the freedom of States to regulate, and the right to protect their cyber infrastructure, persons engaged in cyber activities, and cyber activities located or taking place on their territory. External sovereignty in turn requires States to respect the legal personality, territorial integrity and political independence of other States. In this context sovereignty extends to the physical, logical and social layers allowing States to regulate, for example submarine cables in their territorial sea, security protocols of online services, and the activities of natural and legal persons around online activities. This means States have the freedom to independently engage in foreign relations and cyber activities beyond their territory, provided these are consistent with its international legal obligations (see *Tallinn Manual* (n 95) 11-16).

within their territories, as well as the online activities of people and entities within their jurisdiction. While this may give the impression of an orderly system, scratching the surface shows the complications. For example, it tells us little or nothing about the extent to which a State can regulate the harmful behaviour of people and entities outside their jurisdiction, such as cyber-attacks.

KEY POINT:

States officially articulating their positions on matters such as sovereignty in cyberspace can help develop shared understandings and potentially lead to the development of customary international law.

The current debate about sovereignty in the cyber context largely revolves around the circumstances under which a State's sovereignty is violated by the cyber activities of another State. This debate can be generalised as involving two different positions: the 'sovereignty as a rule' approach and the 'sovereignty as a principle' approach. According to the rule approach, sovereignty operates as a primary rule of international law that can be violated, and under certain circumstances remotely conducted cyber operations can amount to violations of sovereignty. The sovereignty as a principle approach in turn is premised on the view that sovereignty does not operate as a standalone rule of international law independent from the non-use of force and non-intervention principles, but instead operates as a principle that underpins these rules. This means that there cannot be a violation of sovereignty independent of a violation of another rule of international law that is premised on the principle of sovereignty.

The sovereignty as a rule approach has attracted most support from States so far. This is the approach that has been adopted by the Netherlands,[100] Switzerland,[101] France,[102] Austria,[103] the Czech

[100] Letter from the Government of the Kingdom of the Netherlands, Minister of Foreign Affairs to Parliament, July 2019, 2 https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/02/appendix-Internaional-law-in-cyberspace-kingdom-of-the-netherlands.pdf (*'The Netherlands letter'*).

[101] Switzerland's position paper on the application of international law in cyberspace, Annex UN GGE 2019/2021, 2-3 <https://www.dfae.admin.ch/dam/eda/en/documents/aussenpolitik/voelkerrecht/20210527-Schweiz-Annex-UN-GGE-Cybersecurity-2019-2021_EN.pdf>.

[102] UN Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security: Report of the Secretary-General*, UN Doc A/74/120 (24 June 2019) 22-6 (*'UN Developments 2019'*).

[103] Austria maintained that 'a violation of the principle of State sovereignty constitutes an internationally wrongful act'. 'Comments by Austria, Pre-Draft Report of the OEWG – ICT' (31 March 2020) https://front.un-arm.org/wp-content/uploads/2020/04/comments-by-austria.pdf (*'Austria comments'*).

Republic,[104] Finland,[105] Iran,[106] Germany,[107] and arguably New Zealand.[108] However, despite the consensus among these States that sovereignty operates as a primary rule that can be violated, their positions differ or are silent on the circumstances in which sovereignty is violated. This is a crucial distinction to make as, for example, the French and Iranians positions suggest that these States would consider any unauthorised penetration of their systems a violation of sovereignty, whereas for others States such as New Zealand cyber espionage and even cyber operations with some effects are not considered to be in violation of sovereignty (this is similar to the position of those States adopting the 'sovereignty as a principle' approach).

Most academic commentators support this view, though here too there is divergence on the threshold question.[109]

The sovereignty as a principle approach has been taken expressly by the UK, the US has alluded to this view, and some academic commentators support this position. According to this approach, sovereignty is a fundamental principle of international law and involves an internal element (the independent right to exercise State functions to the exclusion of others) and an external element (the recognition of the absolute equality and independence of all States).[110] But sovereignty cannot be violated in its own right independent of other rules of international law that are based on it as it does not operate as a standalone primary rule of international law capable of being violated. For example, according to the UK position, sovereignty is 'fundamental to the international rules-based system' but there is no 'specific rule or additional prohibition' for cyber activities that fall below the use of force and

---

[104] The Czech Republic noted that it considers 'the principle of sovereignty as an independent right and the respect to sovereignty as an independent obligation.' Czech Republic, 'Statement by Richard Kadlčák at Open-ended Working Group on developments in the field of information and telecommunications in the context of international security of the First Committee of the General Assembly of the United Nations' (11 February 2020) https://www.nukib.cz/download/publications_en/CZ%20Statement%20-%20OEWG%20-%20International%20Law%2011.02.2020.pdf (*'Czech Republic statement'*).

[105] According to Finland, sovereignty is 'a primary norm of public international law, a breach of which amounts to an internationally wrongful act and triggers State responsibility.' Finnish Government, Ministry for Foreign Affairs, 'Finland published its positions on public international law in cyberspace' (15 October 2020) https://valtioneuvosto.fi/en/-/finland-published-its-positions-on-public-international-law-in-cyberspace (*'Finland statement'*).

[106] See Islamic Republic of Iran, 'Declaration of General Staff of the Armed Forces of the Islamic Republic of Iran Regarding International Law Applicable to the Cyberspace' (July 2020) https://nournews.ir/En/News/53144/General-Staff-of-Iranian-Armed-Forces-Warns-of-Tough-Reaction-to-Any-Cyber-Threat ('*Íran declaration*').

[107] Federal Government of Germany, 'On the Application of International Law in Cyberspace' (March 2021), 4 https://www.auswaertiges-amt.de/blob/2446304/2ae17233b62966a4b7f16d50ca3c6802/on-the-application-of-international-law-in-cyberspace-data.pdf (*'Germany statement'*).

[108] New Zealand Foreign Affairs and Trade, 'The Application of International Law to State Activity in Cyberspace' (1 December 2020) https://www.mfat.govt.nz/en/media-and-resources/ministry-statements-and-speeches/cyber-il (*'New Zealand statement'*).

[109] For example, according to Russell Buchan, 'an act of cyber espionage – or indeed any cyber operation – that penetrates computer networks and systems supported by cyber infrastructure situated within the territory of another State constitutes a violation of that State's territorial sovereignty, irrespective of whether that operation causes damage or harm.' Russell Buchan, *Cyber Espionage and International Law* (Hart Publishing, 2019) 54 ('*Buchan*'). Similarly, François Delerue argues that '[i]f a cyber operation penetrates the cyber infrastructures in the territory of a foreign State, this would irrefutably constitute a violation of territorial sovereignty.' Like Buchan, he maintains that there is no requirement for physical damage – he argues that the law does not require any degree of harm and instead that any unauthorised intrusion (whether it is a satellite, ship or plane penetrating another State's territory) is a violation of their territorial sovereignty. Extending this to cyber operations, while those with physical effects are more likely to qualify as violations of territorial sovereignty, he argues that theoretically all cyber operations violate territorial sovereignty but that States do not qualify them as such for political (opposed to legal) reasons. See François Delerue, *Cyber Operations and International Law* (Cambridge University Press, 2020) 214-8 ('*Delerue*'). The Tallinn Manual experts were also divided on this, see *Tallinn Manual* (n 95) 21.

[110] Corn and Taylor (n 47) 209; Jennifer M O'Connor, 'International Law Framework for Employing Cyber Capabilities in Military Operations' (Memorandum, 19 January 2017) 3 ('*O'Connor*').

intervention thresholds.[111] This is because 'there is no such rule as a matter of current international law.'[112] According to the US DoD memo, the law does not presently support the proposition that 'sovereignty acts as a binding legal norm' relevant to cyber activities.[113] Similarly, according to Corn and Taylor, 'sovereignty serves as a principle of international law that guides State interactions, but is not itself a binding rule that dictates results under international law.'[114]

Ultimately, in the cyber context, the key issue of contention between these views surrounds the threshold at which cyber operations violate international law. Consider, for example, a State-sponsored cyber operation that causes damage to computer hardware in another State. For most States and academics adopting the rule approach to sovereignty, this would constitute a violation of territorial sovereignty (on the basis that it causes physical effects within the territory of another State). Depending on the extent of the effects, it could also be regarded as a use of force in violation of article 2(4) of the UN Charter.

In contrast, for those adopting the principle approach to sovereignty, this cyber operation could not constitute a violation of sovereignty as no such rule exists independent of, for example, the prohibition on the use of force. From the UK perspective, for example, this cyber operation may constitute a use of force, but if it falls below this threshold then it would not necessarily be considered in violation of international law, unless it also involved coercion toward the State, in which case it may constitute a violation of the non-intervention principle. As such, ultimately the core question is about what kinds of malicious cyber activities and what threshold of harm is required for a violation of international law to occur. In other words, this raises questions as to what kinds of cyber activities are implicitly permitted under international law provided they remain below certain thresholds in terms of their effects or the harm they cause? These questions remain to be answered by State practice.

KEY POINT:

"...ultimately the core question is about what kinds of malicious cyber activities and what threshold of harm is required for a violation of international law to occur."

The current position of States on sovereignty

As mentioned, a growing number of States have adopted the 'rule approach' to sovereignty in their national views as part of the ongoing UN processes (GGE and OEWG). In 2019, the Netherlands adopted the view that sovereignty is a primary rule

[111] Jeremy Wright, 'Cyber and International Law in the 21st Century' (Speech, Chatham House, Royal Institute of International Affairs, 23 May 2018) <https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century> ('*Wright*').
[112] Ibid.
[113] O'Connor (n 110) 3.
[114] Corn and Taylor (n 48) 208. A third option – in a sense a middle-ground – is presented in Dan Svantesson, 'Lagom Jurisdiction' – What Viking drinking etiquette Can Teach Us About Internet Jurisdiction and Google France' (2018) 12(1) *Masaryk University Journal of Law and Technology* 12(1) 29, 37-39.

of international law that can be violated in its own right.[115] France similarly adopted the view that sovereignty applies as a primary rule of international law, and sovereignty extends to its 'information systems, individuals and cyberspace related activities on its territory'.[116] Subsequently, a number of other States adopted positions along these lines. According to Austria,[117] the Czech Republic,[118] Finland,[119] Iran,[120] Germany,[121] Switzerland,[122] and arguably New Zealand[123] sovereignty operates as a primary rule of international law that can be violated. The Netherlands, for example, while expressing support for the Tallinn Manual experts' approach, stopped short of defining the boundary at which it considers its sovereignty to be violated.[124] Austria similarly remained silent on the circumstances in which it considers sovereignty to be violated.[125] Finland provided that this will be determined on a case-by-case basis depending on the 'nature and consequences' of the unauthorised cyber intrusion.[126]

However, among these States there is divergence in views about the threshold question of when a cyber operation violates sovereignty. While most agree that destructive or deadly cyber operations would violate sovereignty (and possibly other rules of international law), more problematic are those activities below these thresholds. In addition to cyber operations that generate effects within its territory, the French position suggests that it considers a cyber operation that merely involves the 'unauthorised penetration' of its computer systems to be a violation of its sovereignty.[127] Iran's position suggests that it would also view any unlawful intrusions into its (public or private) cyber infrastructure as violations of its sovereignty,[128] as well as those that are destructive or disruptive and undermine its national security.[129] The Czech Republic considers a cyber operation that causes 'death or injury to persons or significant physical damage' to violate its sovereignty; those that damage or disrupt the operation of cyber or other infrastructure and have a 'significant impact on national security, economy, public health or environment';[130] and cyber operations that interfere 'with any data or services which are essential for the exercise of inherently governmental functions, and thereby significantly disrupting the exercise of those functions'.[131] Here it gives the example of 'distributing ransomware which encrypts the computers used by a government and thus significantly delaying the payment of retirement pensions'.[132] According to Germany, a cyber operation that causes

[115] *The Netherlands letter* (n 100). See also The Government of the Kingdom of the Netherlands, *The Netherlands' Position Paper on the UN Open-ended Working Group "on Developments in the Field of Information and Telecommunications in the Context of International Security" and the UN Group of Governmental Experts "on Advancing responsible State Behavior in Cyberspace in the Context of International Security"* (February 2020) 2 <https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/02/letter-to-chair-of-oewg-kingdom-of-the-netherlands.pdf>.
[116] *UN Developments* 2019 (n 102) 22.
[117] *Austria comments* (n 103).
[118] *Czech Republic statement* (n 104).
[119] *Finland statement* (n 105).
[120] *Iran declaration* (n 106).
[121] *Germany statement* (n 107) 4
[122] Switzerland statement (n 101).
[123] *New Zealand statement* (n 108).
[124] *The Netherlands letter* (n 100).
[125] *Austria comments* (n 103).
[126] *Finland statement* (n 105).
[127] *UN Developments 2019* (n 102) 22.
[128] *Iran declaration* (n 106).
[129] Ibid.
[130] *Czech Republic statement* (n 104).
[131] Ibid.
[132] Ibid.

'physical effects and harm' in another State's territory will violate sovereignty, as well as disruptive cyber operations particularly where they cause 'substantive secondary or indirect physical effects' in another State's territory.[133]

From these examples it is clear that States commonly include a 'significance test' in their articulations of what constitutes a violation of sovereignty. Thus, while as noted above it is generally accepted that States have sovereignty over the cyber infrastructure within their territory, it seems to be the case that this sovereignty is only violated if the consequences of the activity in question is sufficiently significant.

From the view of those adopting the 'sovereignty as a principle' approach, sovereignty is not a rule of international law that can be violated by itself. Instead, the cyber operation in question would need to constitute a violation of other existing rules of international law that arise from the principle of sovereignty, such as the prohibition on the use of force or the non-intervention principle.[134] The implication of this is that range of cyber operations are considered lawful under as they are not expressly prohibited under international law. For example, according to the US DoD memo, sovereignty does not limit States from engaging in cyber activities 'that result in effects occurring on the infrastructure located in another State'.[135] Similarly, according to the UK, the non-consensual interference into another State's computer networks is not a violation of their 'territorial sovereignty' because such a rule does not exist in international law in relation to cyber.[136] More recently, however, in 2020 the General Counsel of the US Department of Defence Paul Ney noted that:

> States have sovereignty over the information and communications technology infrastructure within their territory. The implications of sovereignty for cyberspace are complex, and we continue to study this issue and how State practice evolves in this area, even if it does not appear that there exists a rule that all infringements on sovereignty in cyberspace necessarily involve violations of international law.[137]

This can be regarded as a shift away from the UK's strong 'sovereignty as a principle' position as Ney's remarks appear to suggest that, while not all cyber operations infringe sovereignty, there may be some types of operations that may but that this area of law continues to evolve.[138] Notwithstanding this, pursuant to the sovereignty as a principle approach, unauthorised cyber intrusions cannot constitute violations of sovereignty (because no such rule exists) and will only amount to violations of international law where they rise to the threshold of a use of force or intervention and thus violate other existing rules of international law.

Given that the States that adhere to the sovereignty as a rule perspective commonly include a 'significance test' in their articulations of what constitutes a violation of sovereignty, perhaps the two positions are not that different after all. In the end, whether one takes the view that

---

[133] *Germany statement* (n 107) 4
[134] Corn and Taylor (n 47) 208.
[135] O'Connor (n 110) 3.
[136] United Kingdom of Great Britain and Northern Ireland, *Non-Paper on Efforts to Implement Norms of Responsible State Behaviour in Cyberspace, as Agreed in UN Group of Government Expert Reports of 2010, 2013 and 2015* (September 2019) 11 <https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/09/uk-un-norms-non-paper-oewg-submission-final.pdf>.
[137] Paul C. Ney Jr, 'DOD General Counsel Remarks at U.S. Cyber Command Legal Conference' (2 March 2020) <https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference>.
[138] See also See Marko Milanovic and Michael Schmitt, 'Cyber Attacks and Cyber (Mis)information Operations During a Pandemic' (2020) 11 *Journal of National Security Law and Policy* 247, 252-3.

sovereignty is a rule that is violated if the consequences of the activity in question is sufficiently significant, or whether one takes the view that sovereignty is a principle and that the threshold stems from a 'use of force' or 'intervention' focused test a similar assessment may perhaps be made in any given situation.

In late 2020, New Zealand also outlined its position including details about the threshold question of when it considers a cyber operation to violate sovereignty. New Zealand's position is unique as it notes how sovereignty as a 'principle' has legal effect through the prohibition on the use or force and intervention, but also that a 'standalone rule of territorial sovereignty also applies in the cyber context'.[139] As such, New Zealand seemingly adopts both the principle and rule approach to sovereignty. As to when sovereignty is violated, it maintains that this occurs where a State uses 'cyber means to cause significant harmful effects manifesting on the territory of another State.'[140] This in turn requires consideration of 'the scale and significance of the effects, the objective of the activity, and the nature of the target.'[141] Here New Zealand makes it clear that it does not consider 'every unauthorised intrusion' into another State's ICT systems or even all cyber activities causing effects on another State's territory to be a violation of territorial sovereignty.[142] It notes that in addition to 'pure espionage activity' there are a range of circumstances 'in which an unauthorised cyber intrusion, including one causing effects on the territory of another State, would not be internationally wrongful.'[143] Here it provides the example where a State takes 'necessary measures, with minimally destructive effects, to defend against the harmful activity of malicious cyber actors in another State.[144] As such, while New Zealand expressly confirms the rule approach to sovereignty, the threshold at which it considers sovereignty to be violated is akin to those adopting the principle approach.

Accordingly, most States that have expressed their legal position have adopted the view that sovereignty operates as a rule of international law that can be violated by cyber operations. However, the threshold at which this occurs remains disputed but generally this is likely to be assessed on a case-by-case basis depending on the nature, circumstances and consequences of the cyber operation.

The non-intervention principle

The non-intervention principle is closely connected with State sovereignty and the respect for sovereignty of other States. It is a rule of customary international law that prohibits States from using coercive means to intervene in the internal or external affairs – matters which States have the right to decide freely by virtue of their

[139] *New Zealand statement* (n 108).
[140] Ibid.
[141] Ibid.
[142] Ibid.
[143] Ibid.
[144] Ibid.

sovereignty. For those adopting the 'sovereignty as a rule approach', the non-intervention principle mainly captures cyber operations that violate sovereignty but are also coercive in nature and seek to undermine these matters. For those adopting the 'sovereignty as a principle approach', the non-intervention principle provides the lowest threshold for cyber operations for cyber operations to constitute violations of international law (ie. generally cyber activities that do not rise to the level of an intervention would not be considered in violation of international law).

The non-intervention principle was framed in the 1970 UNGA Declaration on Friendly Relations in the following terms:

> No State or group of States has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State. Consequently, armed intervention and all other forms of interference or attempted threats against the personality of the State or against its political, economic and cultural elements, are in violation of international law.[145]

Historically the non-intervention principle was only considered relevant in relation to 'forcible or dictatorial' interference – that is, mainly interventions involving the use of force.[146] In the modern context, however, a violation of the non-intervention principle does not require a use of force (though any use of force is considered to also constitute an intervention).[147] The ICJ in the 1986 Nicaragua case discussed the principle of non-intervention stating that:

> A prohibited intervention must accordingly be one bearing on matters in which each State is permitted, by the principle of State sovereignty, to decide freely. One of these is the choice of a political, economic, social and cultural system, and the formulation of foreign policy. Intervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones. The element of coercion, which defines, and indeed forms the very essence of, prohibited intervention, is particularly obvious in the case of an intervention which uses force[.][148]

As such, the non-intervention principle contains two elements. First, there must be coercive interference, and second, it must be directed towards the matters that sovereign States should be able to decide freely.[149]

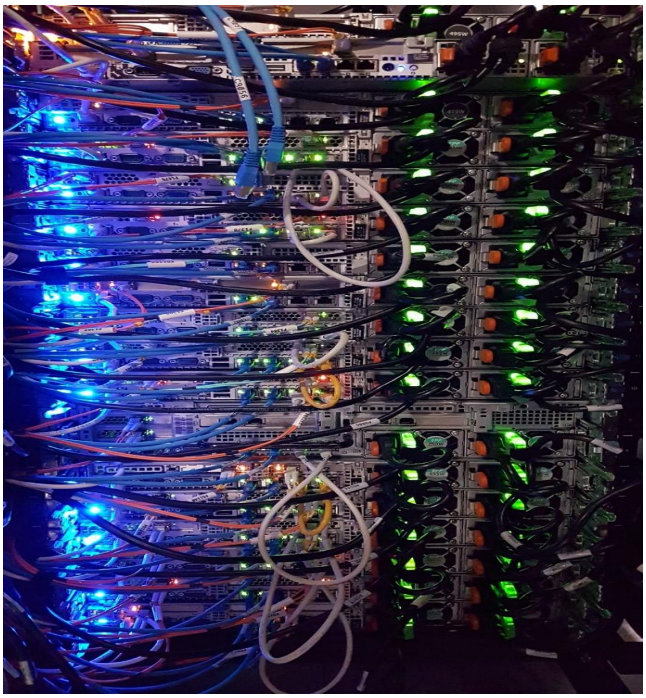
The notion of coercion is not defined under international law. The majority of the Tallinn Manual experts, for example, defined it as 'an affirmative act designed to deprive another State of its freedom of choice, that is, to force that State to act in an involuntary manner or involuntarily refrain from acting in a particular way.'[150] As such, they maintained that it requires more than other types of pressures involving influencing (opposed to factually compelling) the behaviour of a State, such as public criticism, propaganda, or persuasion.[151] Other academic

---

[145] UNGA Res 2625 (XXV), UN Doc A/RES/2625(XXV) (24 October 1970) 123.
[146] Robert Y Jennings and Arthur Watts (eds), *Oppenheim's International Law, Volume 1, Peace* (Longman, 9th ed, 1992) 430 (*'Jennings and Watts'*) cited in David J Harris, *Cases and Materials on International Law* (Thomson Reuters, 7th ed, 2010) 743. See also Lori F Damrosch, 'Politics Across Borders: Nonintervention and Nonforcible Influence Over Domestic Affairs' (1989) 83 *American Journal of International Law* 1, 3.
[147] According to the ICJ, activities involving the use of force would be 'wrongful in the light of both the principle of non-use of force, and that of non-intervention.' *Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v United States of America)* (Merits) [1986] ICJ Rep 14, 108 (*'Nicaragua v United States of America'*). This was affirmed by the ICJ in *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v Uganda)* [2005] ICJ Rep 168, 227.
[148] *Nicaragua v United States of* America (n 147) 108.
[149] Maziar Jamnejad and Michael Wood, 'The Principle of Non-Intervention' (2009) 22(2) *Leiden Journal of International Law* 345, 347.
[150] *Tallinn Manual* (n 95) 317 citing Jennings and Watts (n 146) 430-431.
[151] *Tallinn Manual* (n 95) 318.

commentators, in light of existing law in this context, have described it more broadly as a form of pressure that seeks to deprive the target State of its free will.[152] Similarly, a minority of the Tallinn Manual experts maintained that it is sufficient that the activity 'has the effect of depriving the State of control over the matter in question.'[153] These broader accounts of coercion are also consistent with Australia's position, according to which coercion involves 'effectively depriv[ing] another State of the ability to control, decide upon or govern matters of an inherently sovereign nature'.[154] This broader account of coercion is preferred over the narrow approach to coercion which requires a State to be forced to act (or not act) in a particular way.

The matters that States are able to decide freely by virtue of their sovereignty are, according to the ICJ, their 'choice of a political, economic, social and cultural system, and the formulation of foreign policy.'[155] This definition is supported by Australia's current position on the law which refers to these as 'matters of an inherently sovereign nature' that sovereign States are permitted to decide freely.[156] The UK and the US also adopt similar language in their legal positions. The concept of domaine réservé ('reserved domain') is often used to refer to matters within the exclusive domestic jurisdiction of States,[157] and sometimes distinguished from the broader State functions that States have the authority to exercise.[158] However, instead of this concept, the notion of 'matters in which each State is permitted, by the principle of State sovereignty, to decide freely' (using the ICJ's wording) is preferred. It is not confined to a State's internal affairs as it also includes their external affairs (eg. membership of international organisations, and decisions to recognise States). Similarly, even if a matter is regulated by international law (and thus it is no longer within its domaine réservé meaning the State no longer has exclusive regulatory authority over the matter), it still has the authority to make choices within that area of law.[159] As such, the 'matters that sovereign States are permitted to decide freely' is a more useful concept opposed to the narrow notion of a



[152] Moynihan (n 97) 30 ('pressure applied by one State to deprive the target State of its free will in relation to the exercise of its sovereign rights in an attempt to compel an outcome in, or conduct with respect to, a matter reserved to the target State.')
[153] *Tallinn Manual* (n 95) 318.
[154] Department of Foreign Affairs and Trade, *Australia's International Cyber Engagement Strategy (*2019 International Law Supplement) https://www.dfat.gov.au/publications/international-relations/international-cyber-engagement-strategy/aices/chapters/2019_international_law_supplement.html ('*Australia's International Cyber Engagement Strategy 2019*').
[155] *Nicaragua v United States of* America (n 147) 108.
[156] Australia's International Cyber Engagement Strategy 2019 (n 154).
[157] See Katja Ziegler, 'Domaine Réservé' in *Max Planck Encyclopaedia of Public International Law* (Oxford University Press [online] 2013).
[158] The Tallinn Manual, for example, distinguishes a State's 'inherently governmental functions' (relevant for a sovereignty violation) from the concept of *domaine reserve* (relevant to the non-intervention principle). *Tallinn Manual* (n 95) 24.
[159] See Moynihan (n 97) 34.

State's domaine réservé.[160] There is widespread agreement among States that the non-intervention principle is applicable in the cyber context.[161] The Tallinn Manual also provides in Rule 66 that States 'may not intervene, including by cyber means, in the internal or external affairs of another State.'[162]

KEY POINT:

There is widespread agreement among States that the non-intervention principle is applicable in the cyber context.

A number of States have outlined their positions on this and detailed when they consider the principle to have been violated. For example, according to the UK and Australia, a prohibited intervention occurs where a State uses cyber means to manipulate another State's election results, intervene in the operation of its legislative body, or intervene in the stability of its financial system.[163] Finland has similarly recognised the manipulation of vote counts to alter election results as a clear example of a prohibited intervention,[164] And so too has the United States.[165]

The prohibition on the use of force

The prohibition on the use of force is contained within article 2(4) of the UN Charter. It provides that:

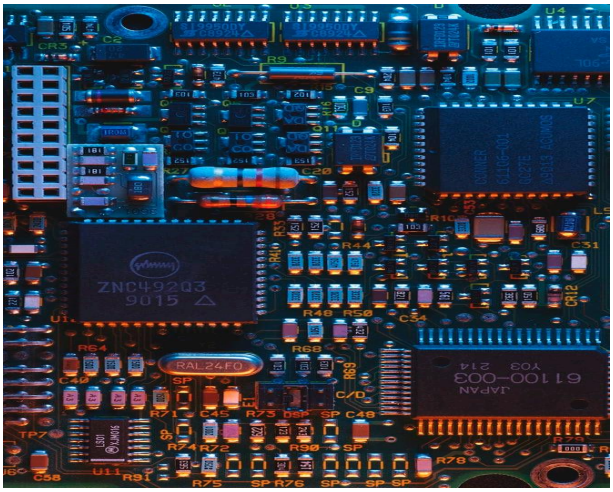
> All Members [of the UN] shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the Purposes of the United Nations.

Within the UN system, the use of force is generally prohibited unless (1) it is in self-defence, (2) it has been authorised by the UN Security Council, or (3) the targeted State consents to it. While article 2(4) was drafted in the technological context of the 1940s, the ICJ has affirmed that it applies 'to any use of force, regardless of the weapons employed.'[166] Article 2(4) also prohibits threats to use force, however, the focus here is on cyber operations that qualify as actual uses of force.[167]

---

[160] See Moynihan (n 97) 34.
[161] *UN GGE Report 2015* (n 91) 12.
[162] *Tallinn Manual* (n 95) 312.
[163] Wright (n 111); Australia's International Cyber Engagement Strategy 2019 (n 154).
[164] Finland statement (n 105).
[165] Brian Egan, 'Remarks on International Law and Stability in Cyberspace' (US Department of State, 10 November 2016) https://2009-2017.state.gov/s/l/releases/remarks/264303.htm ('*Egan*').
[166] *Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion)* [1996] ICJ Rep 226, 244.
[167] On threats to use force, see generally, Albrecht Randelzhofer, 'Article 2(4)' in Bruno Simma and others (eds), *The Charter of the United Nations: A Commentary* (Oxford University Press, 2002) 124-5. According to the Tallinn Manual, a threat of force in the cyber context can involve either using a cyber operation to communicate a threat of a use of force (whether kinetic or cyber), or threats that are conveyed by other means to carry out a cyber operation that rises to the level of a use of force. See Tallinn Manual (n 95) 338. Some argue that large scale Distributed Denial of Service (DDoS) attacks could constitute a demonstration of force and thus constitute a threat to use force, whereas a State merely building its

States have agreed that the UN Charter generally applies to their activities in the cyber context.[168] Many States, including Australia, have taken the approach that a cyber operation constitutes a use of force where its 'scale and effects' are similar to a traditional use of force through kinetic means,[169] thus again adopting a 'significance test'. Other States have taken a similar approach (Netherlands, New Zealand, US). This approach is similar to the one adopted by the Tallinn Manual which provides in Rule 69 that 'A cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force.'[170] As such, where a cyber operation results in damage or destruction of physical property, or injury or death of human beings, it is likely to be considered to amount to a use of force in violation of article 2(4).



The Tallinn Manual provides 8 criteria to aid in the determination of when a cyber operation constitutes a use of force. The Netherlands, for example, has endorsed this criteria as useful in providing 'an indication that a cyber operation may be deemed a use of force'.[171] These criteria are: 1) severity of consequences; 2) immediacy of consequence; 3) directness between the cyber operation as the cause and its effects; 4) invasiveness of the cyber operation into the systems of the targeted State; 5) the measurability of the effects; 6) the military character of the operation; 7) the degree of State involvement in the operation; and 8) the presumptive legality of the operation (whether it involves espionage, for example, which is generally not considered to be expressly prohibited under law).[172]

There is debate about whether a situation where a cyber operation results in loss of functionality of systems (opposed to causing physical damage or harm) would constitute a use of force.[173] From the States that have adopted a position on the application of article 2(4) to cyber operations, only the Netherlands has suggested that 'a cyber operation with a very serious financial or economic impact may qualify as the use of force.'[174] In contrast, New Zealand has maintained that a cyber operation causing significant loss of functionality in its critical infrastructure (eg. financial system, electricity or telecommunications network) would constitute a violation of the non-intervention principle (opposed to a use of force).[175] As such, the law in this context is unclear, but it is possible that where a cyber operation has serious non-physical effects then the victim State may be consider it a use of force.

---

cyber capabilities would not qualify. See François Delerue, *Cyber Operations and International Law* (Cambridge University Press, 2020) 319-26.

[168] *UN GGE Report* 2015 (n 91) 12.

[169] Department of Foreign Affairs and Trade, 'Australia's International Cyber Engagement Strategy' (October 2017) 90 https://www.dfat.gov.au/publications/international-relations/international-cyber-engagement-strategy/aices/index.html ('*Australia's International Cyber Engagement Strategy 2017*').

[170] Ibid 330.

[171] *The Netherlands letter* (n 100).

[172] *Tallinn Manual* (n 95) 334-336.

[173] See generally, Samuli Haataja, *Cyber Attacks and International Law on the Use of Force: The Turn to Information Ethics* (Routledge, 2019) 89-95.

[174] *The Netherlands letter* (n 100).

[175] *New Zealand statement* (n 108).

KEY POINT:

It is important to note that a cyber operation that amounts to a 'use of force' will not necessarily rise to the level of an 'armed attack' which triggers a State's right to use force in self-defence.

It is important to note that a cyber operation that amounts to a 'use of force' will not necessarily rise to the level of an 'armed attack' which triggers a State's right to use force in self-defence.[176] For a cyber operation to constitute an armed attack, most States consider that it would need to cause large-scale loss of human life and/or significant damage to critical infrastructure – ie. a higher threshold of effects is required (eg. Australia: 'large-scale loss of human life and damage to critical infrastructure';[177] France: 'substantial loss of life, significant material damage, insufficient critical infrastructure with significant consequences'[178]).

Examples of specific activities

Disinformation operations

Disinformation operations can be defined as 'false, inaccurate, or misleading information designed, presented and promoted to intentionally cause public harm or for profit'.[179] The cyber context is a powerful enabler of such operations and in recent years these operations have been used to interfere with elections around the world.

Determining the legality of disinformation operations under international law ultimately depends on the measures used in the operation. As such, merely characterising something as a 'disinformation operation' has no legal significance – it is the techniques used in the operation and effects of the operation that are relevant. For example, simply disseminating propaganda or false information online or through State owned media will generally not violate sovereignty or the non-intervention principle. However, where the activity involves cyber operations that disrupt the availability of government services, alter vote counts or cause destructive effects in the real world, then they are likely to amount to violations of the law. As such, disinformation operations can violate the non-intervention principle where they are coercive and targeted at matters that sovereign States are able to decide freely.

Where disinformation operations are used in the context of election interference, the

[176] Most States, and the ICJ have endorsed this distinction. However, according to States such as the US, there is no distinction between a 'use of force' and an 'armed attack'. See Harold Hongju Koh, 'International Law in Cyberspace' (Speech, USCYBERCOM Interagency Legal Conference, 18 September 2012) <https://2009-2017.state.gov/s/l/releases/remarks/197924.htm> ('*Koh speech*').
[177] Australia's International Cyber Engagement Strategy 2019 (n 155).
[178] *UN Developments 2019* (n 102) 22.
[179] European Commission, 'A Multi-Dimensional Approach to Disinformation: Report of the Independent High Level Group on Fake News and Online Disinformation' (Publications Office of the European Union, 2018) 10 <https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation>. The harm in this context can be to 'democratic political processes and values' and 'a variety of sectors, such as health, science, education, finance and more'.

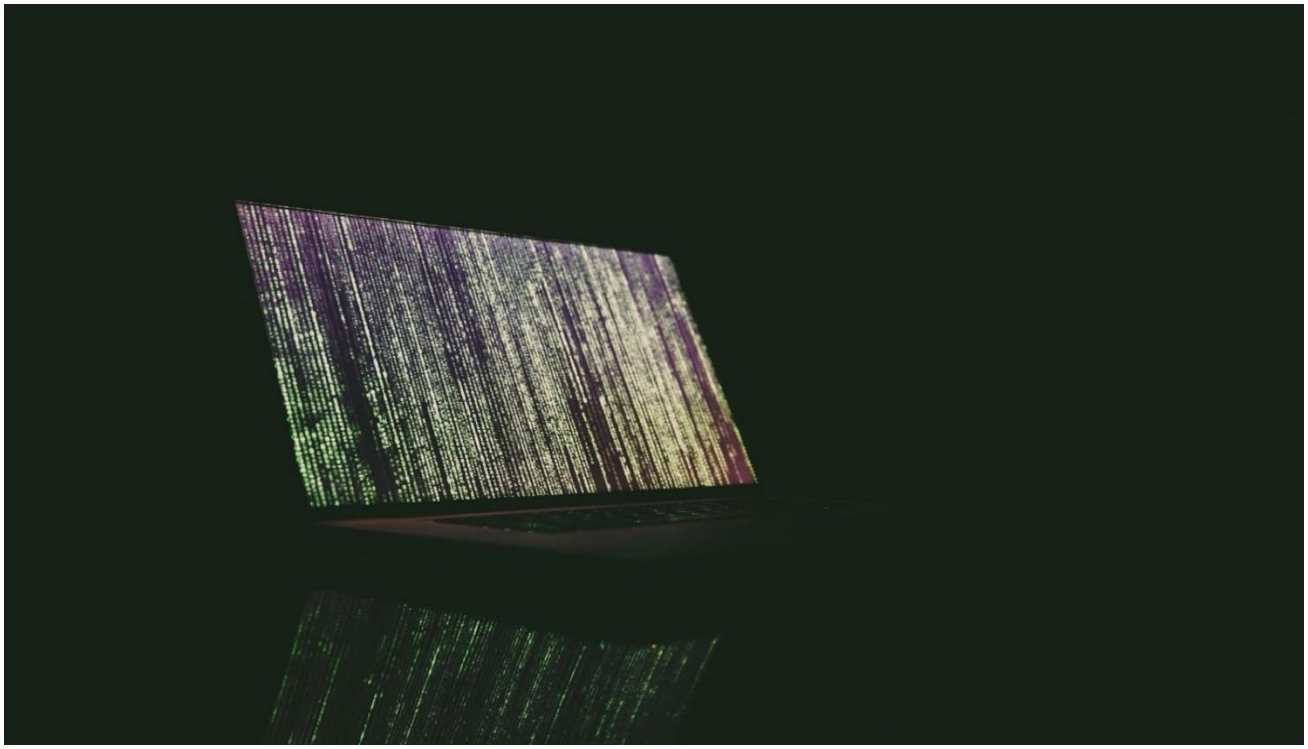
requirement for such operations to be 'coercive' is problematic under existing law. If a narrow definition of coercion as requiring a State is 'compelled' to act in a particular way (or refrain from doing so), then it is difficult to demonstrate that a disinformation operation had this effect. For example, even if a disinformation operation was successful in shaping the views of voters, it would be difficult to demonstrate that it caused them to vote in a particular way which changed the result of the election. In contrast, where disinformation operations involve other forms of cyber enabled election interference (such as cyber operations used to alter vote counts and change the result of the election), then this would generally be considered to constitute a violation of the non-intervention principle.[180] This is on the premise that elections are part of a State's political process and choice of their political system (and thus a matter they can determine freely), and manipulating the election result would involve effectively depriving the target State of the ability to control this process. Vote manipulation like this is considered by many States as an example of what would amount to a violation of the non-intervention principle.[181]

Outside election result manipulation, very few States have outlined their positions on the circumstances in which they consider 'disinformation operations' to violate international law. As mentioned, generally this will depend on the types of cyber operations that are used and their effects. However, New Zealand has provided the example of a 'prolonged and coordinated cyber disinformation operation that significantly undermines a State's public health efforts during a pandemic' as an activity that it would consider to be in violation of the non-intervention principle.[182] A State's public health efforts (eg. regulating its hospitals and the healthcare sector) would fall within matters that sovereign States can decide freely, and during a pandemic these efforts may involve coordinating the national response, healthcare resources, as well as vaccine research and distribution. Where the cyber operation in question is intended to deprive another State of the ability to decide or govern these matters, it could be regarded as a violation of the non-intervention principle.

KEY POINT:

"...disinformation operations can violate the non-intervention principle where they are coercive and targeted at matters that sovereign States are able to decide freely ... a disinformation operation will not constitute a use of force in violation of article 2(4) unless part of the operation involves cyber operations with physical effects (damage, destruction, death, injury)."

[180] See also Michael N Schmitt, 'Virtual Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law' (2018) 19(1) *Chicago Journal of International Law* 30, 50.
[181] *Australia's International Cyber Engagement Strategy 2019* (n 154); Wright (n 111); Egan (n 165).
[182] *New Zealand statement* (n 108).



A disinformation operation could potentially be used to cause these effects, but it would depend on the techniques involved. For example, merely disseminating false information relating to the pandemic or discouraging people from getting vaccinated would unlikely suffice as depriving the State of the ability to control this process or decide these matters, whereas disrupting the operation of vaccine research centres within hospitals with the intention of significantly undermining the State's public health efforts likely would. However, the latter would likely require different types of cyber operations to be used (eg. a Distributed Denial of Service (DDoS) attack) instead of mere disinformation operations involving the dissemination of information.

Similarly, depending on the techniques involved in the disinformation operation, it could constitute a violation of sovereignty. This however also depends on the State's approach to sovereignty. If the disinformation operation merely involves dissemination of false information through social media channels then the activity, in itself, would not constitute a violation of sovereignty. However, should the operation involve disruption to government services (eg. compromising Australia's MyGov service, disruption of its operation, and using it to distribute false information in a way that appears the Government is distributing the information) then many States adopting the rule approach to sovereignty at least would likely consider it a violation of sovereignty (the activity may also violate the non-intervention principle provided it involves coercion). Again, to achieve these effects, it is likely that other techniques are used more than mere dissemination of information.

Finally, a disinformation operation will not constitute a use of force in violation of article 2(4) unless part of the operation involves cyber operations with physical effects (damage, destruction, death, injury). These effects are highly unlikely to occur as a direct result of the dissemination of information and instead other technical means would need to be used in the cyber operation.

Cyber espionage

Cyber espionage generally refers to the use of cyber means to copy confidential data from computer systems or networks without authorisation.[183] As such, cyber espionage does not involve altering or deleting data, disrupting the operation of computer systems or networks, or destructive effects on computer systems.

International law is relatively clear that espionage is permitted in times of war. Indeed, with some exceptions, international law expressly allows wartime espionage. In contrast, peacetime espionage has gained limited attention in international law. In fact, while espionage is criminalised in the domestic legal systems of States, in peacetime under public international law, the law is considered largely silent on espionage conducted by States.[184] Consequently, the uncertainty and complexity that dominates the discussion of peacetime espionage is not merely a cyber issue, it is also applicable to such espionage more broadly.

This means that unless there is a specific prohibition on the activity in question (eg. under the law protecting diplomats and consulates),[185] then States are freely permitted to engage in these activities. As a result of this, determining whether 'cyber espionage' violates international law will depend on the techniques involved and the effects caused by the operations.[186]

Iran's and France's positions on sovereignty appear to suggest that any penetration of their networks would constitute a violation of sovereignty. From this approach, by implication, any act of cyber espionage that involves unauthorised access to computer systems or networks in those States would constitute a violation of sovereignty. Some academic commentators also support this view.[187]

The more dominant view, however, would not regard remotely conducted cyber espionage as a violation of sovereignty, unless the activity involved more than mere information collection. For example, where a cyber espionage operation targets the confidential information of a government department, but in the course of the operation causes effects that disrupts the operation of the department's computer systems and networks (preventing that department from operating properly), then the cyber operation can be regarded as violating the sovereignty of the State. (Most States adopting the rule approach to sovereignty would likely reach this conclusion, whereas those adopting the principle approach would only consider the activity to violate international law where it also involves coercion – and thus the activity could constitute a violation of the non-intervention principle). New Zealand has also been explicit on this in its legal position noting that 'pure espionage activities' (involving cyber intrusions, even where some effects are caused in the territory of another State) are not prohibited by international law, but that sovereignty can still be violated but this will depend on the scale and significance of the effects caused by the operation.[188]

---

[183] See Buchan (n 109) 17-8.
[184] Katharina Ziolkowski, 'Peacetime Cyber Espionage – New Tendencies in Public International Law' in Katharina Ziolkowski (ed), *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy* (NATO CCDCOE 2013) 430-445; Tallinn Manual (n 95) 25.
[185] See Buchan (n 109) 70-94.
[186] The Tallinn Manual similarly notes that the 'mere characterisation of a cyber operation as espionage or not has no legal significance … [r]ather, one must look to the underlying acts to determine whether the operation in question violates international law' (Tallinn Manual (n 95) 25).
[187] See Buchan (n 109); Delerue (n 109) 214-8.
[188] New Zealand statement (n 108).

For cyber espionage to amount to a violation of the non-intervention principle, the operation would need to target matters States are freely able to determine by their sovereignty, and involve coercion. While cyber espionage operations targeting a State's government departments (such as Defence) satisfy the former, the mere copying of confidential information does not deprive the target State of the ability to control, decide, or govern matters it has the sovereign right to. As such, it would not involve the requisite degree of coercion. Therefore, normally cyber espionage will not violate the non-intervention principle as the mere copying of confidential information is not coercive.

Cyber espionage involves the copying of confidential data and does not involve physical effects (such as damage or destruction of computer hardware, or injury or death to human beings). Therefore, cyber espionage activities will normally not constitute a use of force in violation of article 2(4) of the UN Charter.

Cyber-attacks

The Australian Government defines a cyber-attack as 'a deliberate act through cyberspace to manipulate, disrupt, deny, degrade or destroy computers or networks, or the information resident on them, with the effect of seriously compromising national security, stability or economic prosperity.'[189] It is important to note that 'cyber-attack' in this context is a descriptive term and is not a legal concept. The Australian definition also qualifies cyber-attacks based on their effects – the cyber-attack must seriously compromise national security, stability or economic prosperity. Thus, also here, the theme of a 'significance test' is clear.

However, for the purposes of this Report, it is more useful to consider cyber-attacks as 'a deliberate act through cyberspace to manipulate, disrupt, deny, degrade or destroy computers or networks, or the information resident on them' (ie. without qualifying such attacks based on their effects are serious and compromise national security etc). This allows for consideration of the technical effects of cyber-attacks and the legal significance of those effects.

In light of this definition, where a cyber-attack involves physical effects (eg. destroying computer hardware or other physical objects operated by the hardware, or injury or death to human beings) it will generally be considered to constitute a use of force. Under international law, any use of force against another State also constitutes a violation of that State's sovereignty and a violation of the non-intervention principle.[190] As mentioned above, most States have endorsed a 'scale and effects' approach to determining this (and the 8 quantitative and qualitative factors from the Tallinn Manual can be useful in this context) but there is no clear threshold about when a cyber-attack constitutes a use of force. Common examples provided by States of where a cyber-attack amounts to a use of force is where it causes injury or death to human beings;[191] damage to physical objects (though the threshold of damage is uncertain);[192] and damage to critical infrastructure.[193]

[189] *Australia's International Cyber Engagement Strategy 2017* (n 169).
[190] The ICJ in *Nicaragua* noted how any activities involving the use of force would be 'wrongful in the light of both the principle of non-use of force, and that of non-intervention *(Nicaragua v United States of America* (n 147) 108).
[191] *Australia's International Cyber Engagement Strategy 2017* (n 169); Kersti Kaljulaid, 'President of the Republic at the opening of CyCon 2019' (Speech at the CyCon 2019, Tallinn, 29 May 2019) <https://www.president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/index.html> ('*Kaljulaid*').
[192] Australia's International Cyber Engagement Strategy 2017 (n 169) 90; Kaljulaid (n 191).
[193] Australia's International Cyber Engagement Strategy 2017 (n 169).

Examples given by the US of cyber-attacks amounting to a use of force are those that 'trigger a nuclear plant meltdown', 'open a dam above a populated area causing destruction', and 'disable air traffic control resulting in airplane crashes'.[194] It is important to note that, notwithstanding the reasoning of the ICJ in the Nicaragua case, the US does not consider there to be a distinction between a 'use of force' and an 'armed attack' – but these are examples that would undeniably amount to a 'use of force' and an 'armed attack' (allowing a State to respond with force in self-defence) under existing law.[195]

New and emerging conceptions of sovereignty

The discussion above has been focused on the application of the traditional concept of sovereignty in the cyberspace context. However, in addition there is an ongoing discussion of specific sovereignty-related concepts including the following:

1. Digital sovereignty;
2. Technological sovereignty;
3. Cyber sovereignty;
4. Data sovereignty; and
5. Information sovereignty.

To date, a common feature of all these concepts is that they lack legal definitions. Indeed, there is an apparent lack of consensus about their general meanings, their relationship to each other and their relationship to conventional notions of sovereignty.

What is clear, however, is that claims such as claims of digital sovereignty and claims of data sovereignty are powerful political rallying calls pursued both by democratic and by authoritarian States. Some of the motivations for claims of digital, or data, sovereignty are the same for both democratic and authoritarian States. For example, claims of the mentioned types of sovereignty is commonly justified by reference to independence and control. A July 2020 publication by the European Parliament Think Tank is illustrative when it states that, in the European Union context, 'digital sovereignty' refers to: 'Europe's ability to act independently in the digital world and should be understood in terms of both protective mechanisms and offensive tools to foster digital innovation (including in cooperation with non-EU companies)'.[196] The civilian nature of this statement is clear not least from its context being articulated by the EU. However, at the same time, the defence implications are both obvious and overlapping – in the context of digital sovereignty, sharp lines cannot be drawn between civilian and military interests. This is especially so when digital sovereignty is discussed in the context of cyber-resilience or in the context of States reserving the right to respond to hostile activities – two common motivations for calls for digital sovereignty.

A final note should be made in this brief discussion of such calls for sovereignty in the cyberspace context. States such as China and Russia have been calling for cyber sovereignty – seemingly in a coordinated manner – for some time. For example, President Xi Jinping has been calling for 'cyber sovereignty' at least since 2015,[197] and 'the need to establish a clearly demarcated 'national Internet segment' subject to strong governmental oversight

[194] Koh speech (n 176).
[195] Ibid.
[196] Tambiama Madiega, 'Digital sovereignty for Europe' (Briefing, No PE 651.992, European Parliamentary Research Service Ideas Paper, July 2020).
[197] William J. Drake, Vinton G. Cerf and Wolfgang Kleinwachter, 'Internet Fragmentation: An Overview' *World Economic Forum* (January 2016) 46 http://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf.

has been an increasingly consistent theme of Russian policy pronouncements at both the domestic and international levels in recent years.'[198] One potential outcome of the type of sovereignty these States seek is the risk of what has been termed 'fragmentation' of the Internet. Put simply, there may no longer be one coordinated Internet but rather smaller State-based internets with more or less open connections between them. Such a development would have obvious defence implications. Indeed, China – as part of its belt and road project are building extensive Internet architecture that could be used to facilitate an alternative network structure.[199]

KEY POINT:

"In the context of digital sovereignty, sharp lines cannot be drawn between civilian and military interests."

A particular manner in which States are pursuing sovereignty, or perhaps more specifically digital or data sovereignty, in the cyberspace context is through so-called 'data localisation requirements'. A 2020 OECD report defines data localisation in the following manner: "Data localisation' refers to a mandatory legal or administrative requirement directly or indirectly stipulating that data be stored or processed, exclusively or non-exclusively, within a specified jurisdiction."[200]

This definition is not uncontroversial, and some definitions are broader in scope. The important aspect for our purposes is found in the fact that data localisation requirements may be seen as an aspect of the pursuit of data, information and/or technological sovereignty. Put simply, by ensuring that data are stored and processed locally, a degree of control is created that may facilitate the type of cyber resilience that forms part of the calls for digital sovereignty.

At the same time, as is highlighted, for example, in a Canadian discussion of data sovereignty, data localisation may be an ineffective measure to ensure data sovereignty:

> In the public cloud environment, government data is entrusted to a third party that may be subject to the laws of a foreign country, even if the data resides in Canada. As such, the key risk to the GC [Government of Canada] with respect to data sovereignty is that foreign agencies can leverage laws in their home country to compel CSPs [cloud service providers] to turn over the GC's data.[201]

[198] Ibid 45.
[199] Robert Greene and Paul Triolo, 'Will China Control the Global Internet Via its Digital Silk Road?', *Carnegie Endowment for International Peace* (8 May 2020) <https://carnegieendowment.org/2020/05/08/will-china-control-global-internet-via-its-digital-silk-road-pub-81857>.
[200] Dan Svantesson, 'Data Localisation Trends and Challenges: Considerations for the Review of the Privacy Guidelines' (2020) 31, *OECD Digital Economy Papers* 8 <https://doi.org/10.1787/7fbaed62-en.
[201] Treasury Board of Canada Secretariat, *Government of Canada White Paper: Data Sovereignty and Public Cloud* (2018) <http://publications.gc.ca/collections/collection_2018/scttbs/BT22-213-2018-eng.pdf>.

Concluding remarks regarding sovereignty in the cyberspace context

Despite debate about whether sovereignty operates as a 'rule' or a 'principle' in the cyber context – with most States now adopting the view that it operates as a rule – there remains uncertainty about the threshold at which a cyber operation will violate sovereignty. Generally, cyber operations that involve espionage or do not cause effects in the territory of another State will not be considered violations of sovereignty. It is likely that a violation of sovereignty will be determined on a case-by-case basis, and the more effects it causes (such as physical damage or disruption of services) the more likely it may be considered a violation of sovereignty.

From the States that are part of the Five Eyes, the UK has adopted an approach to sovereignty from which States are permitted to engage in range of activities (including cyber espionage) without these activities violating sovereignty. The US has alluded to a similar position, and New Zealand has also adopted an approach that is similar in effect. According to New Zealand, while cyber operations can under certain circumstances violate sovereignty, States can engage in cyber espionage and even cyber operations that cause effects in the territory of another State without violating sovereignty. On the other hand, Australia and Canada have not adopted official positions on how sovereignty applies in the cyber context, and whether and what kinds of it cyber operations are prohibited below the use of force and non-intervention thresholds.

Accordingly, given the current uncertainty in the law surrounding sovereignty in this context, States are not expressly prohibited from engaging in various low-level cyber activities. However, a degree of consensus is emerging that cyber operations with significant effects that qualify as a use of force, or those that are coercive and directed at matters that sovereign States are able to decide freely and quality as an intervention will violate international law.

CHAPTER 4

The relevance for Defence of the developing concept of sovereignty in the space domain

CHAPTER 4: The relevance for Defence of the developing concept of sovereignty in the space domain

Background 47
Sovereignty in outer space 54
Space as res communis 54
The delineation dilemma: where does space start? 54
Australia's legislative position 57
Sovereign rights in space 61
Sovereign rights over nationals and space objects 61
Sovereign rights to natural resources 62
Sovereign obligations in space 63
Defence implications of sovereignty in outer space 64
Weapons testing and development 64
Competition for natural resources 66
Information and intelligence gathering 69
Conclusion: A strategic role for Australia in space 71

Background

The ongoing militarization and threatened weaponization of space thus represents a significant defence challenge for Australia and other nations. Like cyberspace, outer space is a dual use environment with both State and non-State actors present and both military and civilian applications.

On 4 October 1957, a Soviet space object, Sputnik I, was launched and subsequently orbited the Earth over 1,400 times during the following three-month period. This milestone heralded the dawn of the space age, the space race, and the legal regulation of the use and exploration of outer space. There then followed an intense period of international discussion and consideration of how best to provide for a framework of legal principles to regulate outer space. Ultimately, this gave rise to the five UN Space Treaties currently governing the exploration and use of space: the Outer Space Treaty;[202] the Rescue Agreement;[203] the Liability Convention;[204] the Registration Convention;[205] and the Moon Agreement.[206] Australia is a State party to all five of these treaties.

In essence, the first of these, the Outer Space Treaty, which has been ratified by almost every (major) space-faring country, is a statement of fundamental principles and is an exhortation to good behaviour. The exploration and use of outer space is to be free, in the interests of all countries, and not subject to any 'claim of sovereignty'. The Moon and

[202] Treaty on Principles governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, opened for signature 27 January 1967, 610 UNTS 205 (entered into force 10 October 1967) ('*Outer Space Treaty*'), art. I.
[203] Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space, opened for signature 22 April 1968, 672 UNTS 119 (entered into force 3 December 1968) ('*Rescue Agreement*').
[204] Convention on International Liability for Damage Caused by Space Objects, opened for signature 29 March 1972, 961 UNTS 187 (entered into force 1 September 1972) ('*Liability Convention*').
[205] Convention on Registration of Objects Launched into Outer Space, opened for signature 14 January 1975, 1023 UNTS 15 (entered into force 15 September 1976) ('*Registration Convention*').
[206] Agreement Governing the Activities of States on the Moon and Other Celestial Bodies, opened for signature 18 December 1979, 1363 UNTS 3 (entered into force 11 July 1984) ('*Moon Agreement*').

KEY POINT:

The 1967 Outer Space Treaty provides that the Moon and other celestial bodies are to be used exclusively for peaceful purposes. States are prohibited from placing weapons of mass in destruction in orbit or outer space and the militarization of celestial bodies is forbidden. States are responsible for national space activities and are liable for damage caused by their space objects.

other celestial bodies are to be used exclusively for peaceful purposes. States are prohibited from placing weapons of mass in destruction in orbit or outer space and the militarization of celestial bodies is forbidden. States are responsible for national space activities and are liable for damage caused by their space objects.

The Rescue Agreement requires States to take all possible steps to rescue and assist astronauts in distress and promptly return them to the 'launching authority' and, upon request, to provide assistance in recovering space objects that return to Earth within or outside their territory.

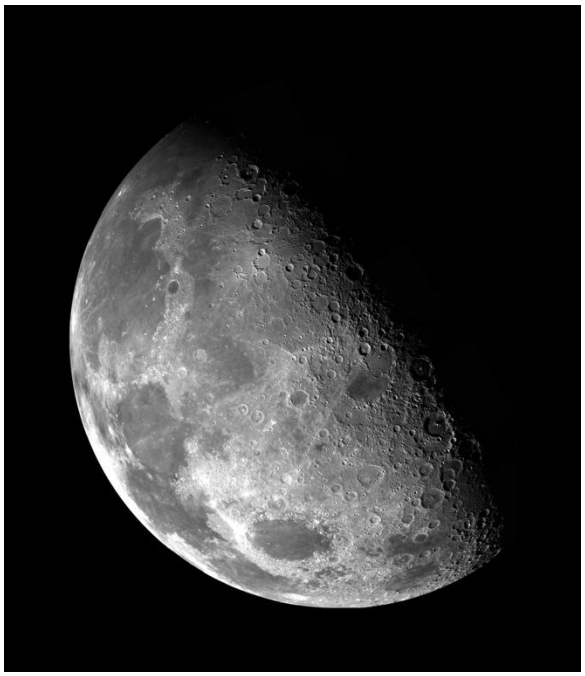
Under the Liability Convention, which also provides for a procedural mechanism for the settlement of sovereign claims for damages, a 'launching State' is absolutely liable to pay compensation for damage caused by its space objects on Earth or to 'aircraft in flight', or on the basis of 'fault' for damage caused elsewhere.

The Registration Convention requires States, and some international organizations, to establish national registries and provide information on their space objects to the Secretary-General of the United Nations. According to the United Nations Office for Outer Space Affairs (UNOOSA), as at 1 January 2019, 89% of all satellites, probes, landers, crewed spacecraft and space station flight elements launched into Earth orbit or beyond have been registered.[207] However, the launch of large constellations of smaller satellites, and the trend towards miniaturization, may challenge this compliance rate in the future.[208] Registration is also initiated voluntarily in accordance with General Assembly Resolution 1721B by States not party to the Registration Convention.

The Moon Agreement both reaffirms and elaborates upon many of the provisions of the Outer Space Treaty relating to the Moon and other celestial bodies, such as its use only being 'exclusively for peaceful purposes', but also expresses that the Moon and its natural resources are the 'common

[207] United Nations Office for Outer Space Affairs, 'United Nations Register of Objects Launched into Outer Space' (Web Page, 1 April 2021) <https://www.unoosa.org/oosa/en/spaceobjectregister/index.html>.
[208] See generally, Steven Freeland, 'Newspace, small satellites, and law: finding a balance between innovation, a changing space paradigm, and regulatory control' in M.T. Adhmad & J. Su (Eds.), *NewSpace Commercialisation and the Law* (McGill University, 2017) 107.

heritage of [hu]mankind' (as interpreted by the States parties to that treaty). It also calls on parties to establish an international regime to govern the exploitation of resources on the Moon and other celestial bodies 'when such exploitation is about to become feasible'.



In addition to the five space treaties, there are also a number of United Nations resolutions, declarations and principles relating to space including: the Declaration of Legal Principles;[209] the Broadcasting Principles;[210] the Remote Sensing Principles;[211] the Nuclear Power Source Principles;[212] and the Benefits Declaration.[213]

Notwithstanding the importance and breadth of these various binding and other instruments, the existing international legal framework does not provide a comprehensive legal set of specific rules for every current (and future) space-related activity, nor for every contingency that may arise. While the fundamental principles in the UN Space Treaties are relevant and applicable to all space activities, it will also be appropriate in certain circumstances to consider other areas of (international) law (such as international criminal law and the law on the threat or use of force) to help resolve a particular dispute, particularly as new and emerging space technologies continue to develop.

That said, apart from the express fundamental principles specified in the UN Space Treaties, the degree to which (general) international law governs outer space is perhaps less straightforward. The Outer Space Treaty affirms that activities in space are to be carried on 'in accordance with international law',[214] but the fact that most existing international law at the time was developed for 'terrestrial' purposes means that it does not expressly contemplate application in outer space. Instead, application of international law by analogy and development of customary international law is required.

Moreover, the traditional non-sovereignty characteristic of outer space meant that any then existent national law (which, in any event, did

[209] *Declaration of Legal Principles Governing the Activities of States in the Exploration and Uses of Space,* GA Res 1962 (XVII) UN GAOR, 18th sess, 1280th plen mtg, Supp No 15, UN Doc A/Res/1962(XVII) (13 December 1963).
[210] *Principles Governing the Use by States of Artificial Earth Satellites for International Direct Television Broadcasting,* GA Res 37/92, UN GAOR, 37th sess, 200th plen mtg, Supp No 51, UN Doc A/37/646 (10 December 1982) ('*Broadcasting Principles*').
[211] *Principles Relating to Remote Sensing of the Earth from Outer Space,* GA Res 41/65, UN GAOR, 41st sess, 95th plen mtg, Agenda Item, Supp NO 53, UN Doc A/RES/41/65 (3 December 1986) ('*Remote Sensing Principles*').
[212] *Draft resolution – Principles Relevant to the Use of Nuclear Power Sources in Outer Space,* GA Res 47/68, 4th Comm, UN DOC A/SPC/47/L.6 (14 December 1992) ('*Nuclear Power Source Principles*').
[213] *Declaration of International Cooperation in the Exploration and Use of Outer Space for the Benefit and in the Interests of All States, Taking into Particular Account the Needs of Developing Countries,* GA Res 51/122, 51st sess, 83rd plen mtg, UN DOC A/RES/51/122 (13 December 1996) ('*Benefits Declaration*').
[214] *Outer Space Treaty* (n 203).

not specifically address space-related issues) would not prima facie apply to this frontier – although, under the international principles of extraterritorial jurisdiction, it might apply to the conduct of a State's nationals,[215] or to its space objects.[216] National law therefore might not be the appropriate legal basis upon which to establish the framework for regulating the conduct of humankind's activities in outer space, although it may be an effective mode for the implementation of international norms once they have been established. It could also be the case that, perhaps, certain international law concepts may provide some regulatory 'models' that might be of interest for the regulation of space activities, at least by way of analogy.

It is also clear that the existing legal and regulatory regime for outer space has not kept pace with the remarkable technological and commercial progress of space activities since 1957. This represents a major challenge in relation to the ongoing development of effective legal principles, all the more in view of the strategic and military potential of outer space in an era of globalisation.
The Outer Space Treaty provides a series of general principles that are intended to restrict the military uses of outer space. As noted, one of these principles is that the requirement 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'.[217] A primary reason for the inclusion of this provision was the concern among many States that outer space would become a new arena for international conflict. In December 1958, the UN General Assembly (UNGA) emphasised the need 'to avoid the extension of present national rivalries into this new field'.[218]

By 1961, the UNGA had recommended that international law and the UN Charter should apply to 'outer space and celestial bodies'.[219] This was repeated in 1963 in UNGA Resolution 1962, which set out a number of important principles that were ultimately incorporated into the Outer Space Treaty.[220] The specific reference to the UN Charter was considered to be important, given that the maintenance of international peace and security is the underlying principle of the system

[215] For a discussion of the possible 'extra-terrestrial' application of national (criminal) law, see Danielle Ireland-Piper and Steven Freeland, 'Star Laws: Criminal Jurisdiction in Outer Space' (2020) 44(1) *Journal of Space Law* 44. See also *Outer Space Treaty* (n 200) art. VIII.
[216] Ibid, *Outer Space Treaty* (n 202).
[217] Ibid, art. III. Article 2 of the *Moon Agreement* (n 206) extends these sentiments further by referring to "the Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations, adopted by the General Assembly on 25 October 1970".
[218] *Question of the Peaceful Use of Outer Space,* GA Res 1348 (XII), UN GAOR, 13th sess, 792nd plen mtg (13 December 1958), Preamble para 3 ('*Question of the Peaceful Use of Outer Space*').
[219] *International co-operation in the peaceful uses of outer space,* GA Res 1721, UN GAOR, 16th sess, Supp NO. 17, 1085th plen mtg, (20 December 1961), par. 1(a).
[220] *Declaration of the Legal Principles Governing the Activities of States in the Exploration and Use of Outer Space,* Ga Res 1962 (XVIII), UN GAOR, 18th sess, 1280th plen mtg, Supp No. 14 (13 December 1963), par. 4.

established under that instrument.[221] The prohibition of the threat or use of force contained in Article 2(4) of the UN Charter represents a crucial element in the regulation of international relations and is equally applicable to the use of outer space.[222]

The sentiments underlying the UN Charter were strengthened further by the restrictions imposed in relation to nuclear weapons and weapons of mass destruction by Article IV of the Outer Space Treaty, although this provision in and of itself does not represent a complete restriction on the placement of weapons in outer space, nor of their use.[223] As noted above, Article IV also provides that '[t]he Moon and other celestial bodies shall be used by all States Parties to the [Outer Space] Treaty *exclusively for peaceful purposes*.'[224]

While there were divergent views as to whether the 'peaceful' use of space was to be interpreted as 'non-military' rather than merely 'non-aggressive' activities,[225] the reality has been that, in addition to the many commercial, civilian and scientific uses, outer space has and continues to be used for an expanding array of military activities. Indeed, the current (geo)political momentum does appear to be directed towards an even greater incorporation of satellite technology in outer space as an integral part of the conduct of warfare.

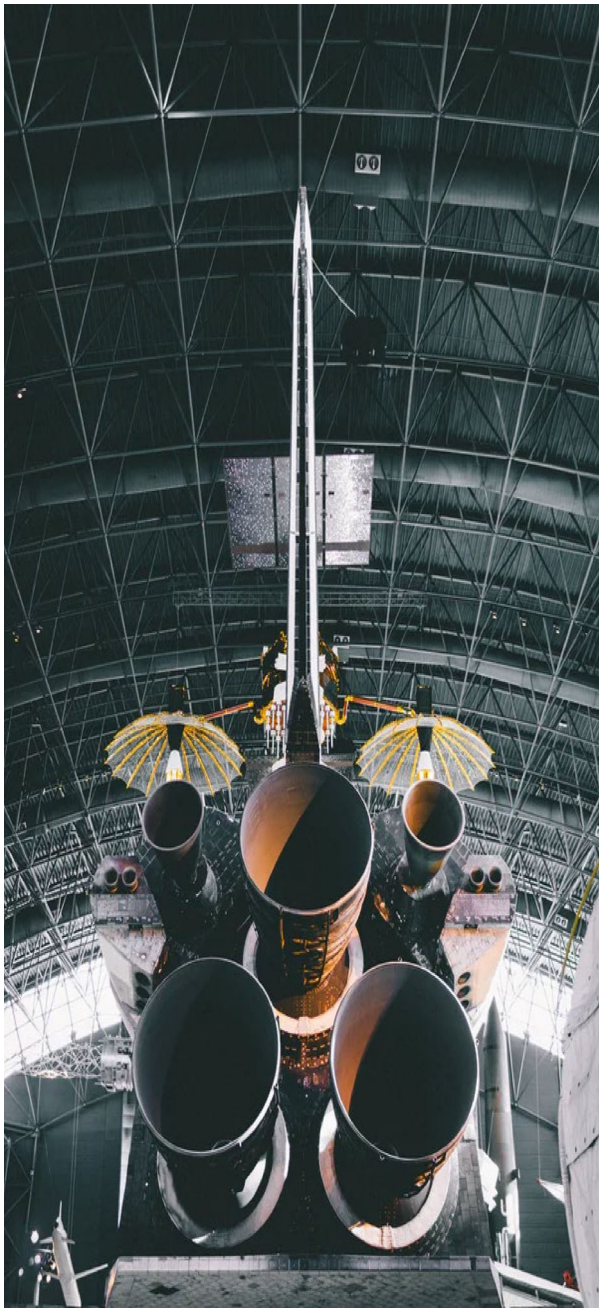
[221] Charter of the United Nations, art. 1(1) ('*UN Charter*'). The first 'Purpose' of the United Nations specified in Article 1(1) of the UN Charter begins with the words: 'To maintain international peace and security …'.
[222] Ibid art. 2(4): 'All Members shall refrain in their international relations 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.'
[223] For a detailed analysis of the *Outer Space Treaty* (n 202), art. IV, see Kai-Uwe Schrogl and Julia Neumann, 'Article IV' in Stephan Hobe, Bernhard Schmidt-Tedd and Kai-Uwe Schrogl (eds), *Cologne Commentary on Space Law, Volume I* (Carl Heymanns Verlag 2009) 70-93.
[224] Emphasis added. See also *Moon Agreement* (n 206) art. 3(1).
[225] For a discussion of the differing interpretations that arose even prior to the conclusion of the Outer Space Treaty, see Bin Cheng, 'The Legal Status of Outer Space and Relevant Issues: Delimitation of Outer Space and Definition of Peaceful Use' (1983) 11:1/2 *Journal of Space Law* 89, 98-101.

KEY POINT:

The use of satellite technology already represents an integral part of the military strategy and the conduct of many armed conflicts. As this technology continues to develop, the armed conflicts of the 21st Century and beyond will increasingly involve the utilisation of outer space.

At present, of the over 190 Member States of the United Nations, approximately 70-80 are engaged in space activities and therefore have domestic capability development to allow them to participate actively in directly accessing space, albeit with varying capacities. This also means that somewhere approaching two-thirds of the world's countries do not have any indigenous space capability whatsoever, placing them at an increasing comparative disadvantage over time and rendering them entirely dependent on others for access to space infrastructure and, indeed, access to space itself.

This gives rise in particular to sovereignty and national security concerns for those States. In addition, the ability to access space and enjoy the benefits in terms of development and the livelihood of those under their jurisdiction is curtailed and highly dependent on strategic and geopolitical networks and understandings. For this reason, we believe that the twin policy for Australia of ensuring access to space through our strategic alliances with certain space-faring nations, whilst also developing further sovereign space capability in specific areas, is essential to Australian national security interests.



The United Nations Committee on the Peaceful Uses of Outer Space (UNCOPUOS), of which Australia is a founding Member State, grew from 24 Member States in 1959 to 96 Member States in 2020. The Organisation for Economic Cooperation and Development (OECD) reports that 'the space sector is currently experiencing an innovation-driven paradigm shift'.[226] In short, the range of activities planned for outer space has expanded as has the range of countries and private entities actively engaged in space activities. This increased use of outer space will likely strain existing legal frameworks, including as they relate to perceptions of sovereignty, sovereign rights and sovereign obligations.

surprising, since the development of space-related technology was, at least initially, inextricably related to military capability – both in reality and to influence the perception of others. In essence, virtually all of the major forms of space technology developed in the first decades after Sputnik 1 were conceived of with military 'eyes'.

It is no coincidence that the space race that began with the Sputnik 1 mission emerged at the height of the Cold War, when both the United States and the USSR strove to flex their respective technological 'muscles'. The early stages of human space activity coincided with a period of quite considerable tension, with the possibility of large scale and potentially

KEY POINT:

The twin policy for Australia of ensuring access to space through our strategic alliances with certain space-faring nations, whilst also developing further sovereign space capability in specific areas, is essential to Australian national security interests.

In addition, and as noted at the outset, the existing legal regime has not prevented the development of military technology capable of utilizing outer space. Whilst there are some restrictions on such technology included in the UN Space Treaties, these were specified in relatively general terms due to the context and geopolitics prevailing at the time they were drafted and have been regarded by some as being open to divergent interpretation as to what they do (and do not) prohibit. This is not entirely

highly destructive military conflict between the (space) superpowers of the time always lurking in the background. Despite the possibilities for science and technology that it would present, the successful launch of Sputnik 1 also generated a sense of significant unease in the West, since the technology used was similar to that for ballistic missiles.[227]

The conventional obligations and restrictions that were eventually agreed and codified in the UN Space Treaties

[226] Organisation for Economic Cooperation and Development, *Space and Innovation* (Report, 27 October 2016).
[227] See, NATO Update, '1957' (Web Page, 2001) <https://www.nato.int/docu/update/50-59/1957e.htm>.

addressed, in part, specific military and weapons-related aspects of space activities. It was, for example, recognised that it was in 'the common interest of all [hu]mankind' that the exploration and use of outer space was to be 'for peaceful purposes'.[228] Whilst initially interpretations of the relevant provisions of this treaty claimed that this prohibited (all) military space activities in outer space, this was not followed by the practice of those States who actually had space capability.[229]

In the specific context of defence applications, therefore, despite legal efforts to make outer space a demilitarized zone, military use of space has been substantial since the beginning of space exploration.

Sovereignty in Outer Space

Space as res communis

Outer space, like the High Seas, is considered in most circles as being akin to a res communis: it belongs to everyone. It is no one State's sovereign territory. It is a key tenet of space law that space is not subject to national appropriation 'by claim of sovereignty, by means of use or occupation, or by any other means'.[230] Specifically, Article I of the Outer Space Treaty provides that the 'exploration and use of outer space, including the moon and other celestial bodies … shall be the province of all [hu]mankind.'[231]

The delineation dilemma: where does space start?

An implication of this res communis characteristic nature of outer space is that the national law of a country does not apply to outer space; rather it is governed and regulated by international law and governance instruments. This immediately raises the question as to where the delimitation is between the airspace above a country (where national law applies) and outer space (where it does not). Prior to the launch of Sputnik 1 in 1957, and the reaction of States to that launch and the orbit of a space object above the Earth, there had been theoretical discussions as to the 'limits'

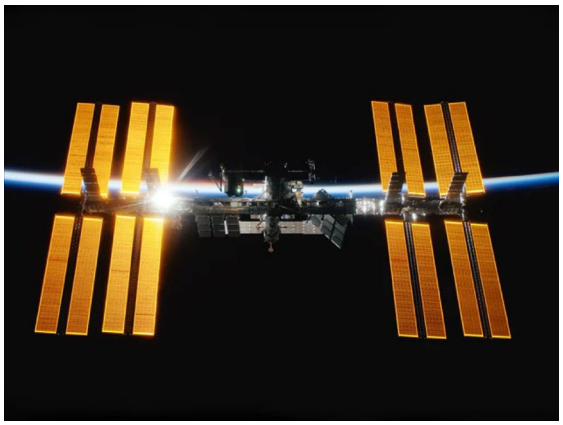
[228] *Outer Space Treaty* (n 201) preamble par. 2. See also *Question of the Peaceful Use of Outer Space* (n 216), passed barely two months after the launch of Sputnik I, where the UNGA recognized that it is 'the common aim that outer space should be used for *peaceful purposes only*' (emphasis added).
[229] See Steven Freeland, 'Applying the *Jus in Bello* to Military Uses of Outer Space: A Square Peg in a Round Hole?' in Patricia Margaret Sterns and Leslie I Tennen (eds), *Private Law, Public Law, Metalaw and Public Policy in Space: A Liber Amicorum in Honor of Ernst Fasan* (Springer 2016) 109.
[230] *Outer Space Treaty* (n 202) art 2.
[231] Ibid art 1.

of upward national sovereignty of a State, with some scholars arguing that a State's sovereignty was without upward limitation – it (in theory) continued 'forever'.[232]

This is not, however, the case. While outer space is - from a practical perspective - generally understood as the area upwards from the airspace (atmosphere) surrounding the Earth, the precise point at which airspace becomes outer space is still the subject of debate. One contributing factor is that the atmosphere does not change dramatically at any certain or consistent height and 'it is impossible to physically determine exactly where the atmosphere ends and outer space begins'.[233]

In many ways, however, the lack of an agreed delimitation is primarily a political (and partially) legal question, rather than a scientific one. The Outer Space Treaty does not define the lower limits of outer space. The major space-faring countries have considered that it is unnecessary to determine a fixed demarcation point, asserting that nothing has turned on the lack of clarity on this point and preferring to retain a 'grey area' approach, thus allowing them to garner competitive advantages over less space-capable countries.

That said, while for some the issue might seem a question of semantics, the boundary is relevant to a number of factors including designation of persons as astronauts for legal purposes. Further, delineation may in certain circumstances represent the difference between an act of space exploration and an act of military



aggression and encroachment of sovereign 'territory'.

There are at least two possible approaches as to when airspace might become outer space. One approach is to simply agree on a particular height/distance at which outer space commences. Suggested distances have included 80 kilometres above sea level due to the composition of the atmosphere at the point, or, for example, 100 kilometres as set out in Australian legislation (see below). Although the position of Australian law is not intended as a formal delineation measure,[234] it is a practical solution given the lack of international consensus on the issue.

Other suggested delineation points include the 'Kármán line'. As at 2021, the 'Kármán line' is set at roughly 100 kilometres above sea level. Another approach is to delineate outer space from airspace by reference to the nature of activities possible in each (aerodynamic lift, for example). However, this would not solve the question in all contexts. For example, the United States Space Shuttle is launched like a rocket but can also use aerodynamic lift like an airplane would when returning to Earth. Therefore, in

[232] For a summary of early approaches to sovereignty as extensive of the upwards "dominance of the State", see: Rhys Monahan, 'The Sky's the Limit? Establishing a Legal Delimitation of Airspace and Outer Space' (Thesis, Durham University, 2008) 1-3.
[233] Lotta Viikari, *The Environmental Element in Space Law* (Martinus Nijhoff Publishers, 2008) 1.
[234] *Space (Launches and Returns) Act 2018* (Cth), s 8.

theory, the Space Shuttle could be governed by both space law and air law, and questions of State sovereignty in airspace might become a complicating factor – in practice, to minimise the complexities, it has been designated as a space object and thus subject to space law. Further:

> Earth's atmosphere doesn't simply vanish; rather, it gradually becomes thinner and thinner over about 600 miles. Technically, the International Space Station - which orbits at an average height of 240 miles - would not be in space if we defined 'space' as the absence of an atmosphere.[235]

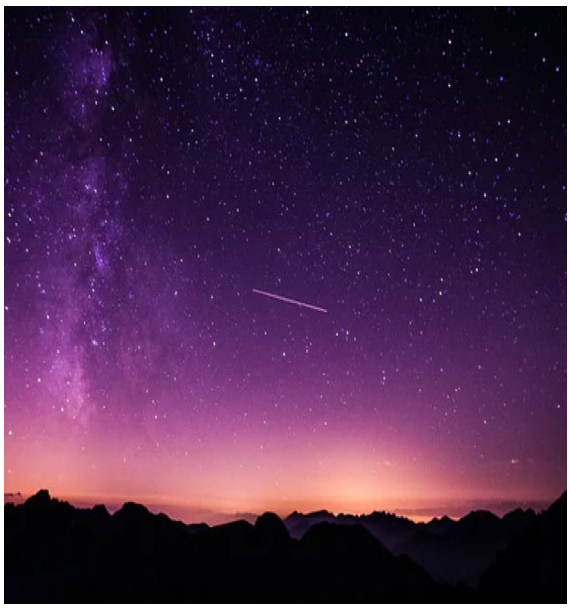
In any event, there is, as noted, currently no agreed definition. As the Legal Subcommittee of UNCOPUOS has observed:

> Since the beginning of its consideration of the question of the definition and delimitation of outer space, in 1967, the Legal Subcommittee has heard diverse views on the issue and considered and addressed numerous proposals received. No agreements on substantive legal issues relating to the definition and delimitation of outer space are apparent from the reports of the Subcommittee or of the Committee on the Peaceful Uses of Outer Space.[236]

The responses by France and Australia to the question as to whether the delineation between outer space and airspace should be defined, well illustrate, by way of example, the continuing debate on the issue:

> The Australian Government recognizes that it is advantageous to domestic entities conducting space activities to have certainty as to the legal framework which applies to their activities. In this respect, the delimitation of activities that must comply with the requirements of the [1998] Space Activities Act and activities that need not comply is necessary for the efficient regulation of domestic Australian space activities. In achieving this goal, the existence of an accepted point of delimitation is more important than the physical location of that point.[237]

France does not consider it appropriate, as the situation with regard to space activities currently stands, to define and delimit outer space. It maintains a functionalist approach to space activities: any object whose purpose is to reach outer space, whether or not that purpose is achieved, is a space object. Thus, the international liability regime established by treaties under the aegis of the United Nations may be applied even when a launched object fails to reach



[235] Nadia Drake, *Where, exactly, is the edge of space? It depends on who you ask*, *National Geographic* (Article, 20 December 2018) <https://www.nationalgeographic.com/science/2018/12/where-is-the-edge-of-space-and-what-is-the-karman-line/>.
[236] Committee on the Peaceful Uses of Outer Space Legal Subcommittee, *Historical summary on the consideration of the question on the definition and delimitation of outer space,* Legal Subcommittee, 41st sess, Agenda Item 6(a), A/AC.105/769 (18 January 2002).
[237] Committee on the Peaceful Uses of Outer Space Legal Subcommittee, *Questions on the definition and delimitation of outer space: replies from Member States: Note by the Secretariat: Addendum*, A/AC.105/889/Add.10 (21 February 2012) 3.

outer space but nevertheless causes damage.[238]

As to legal principles, first and foremost, the journey of Sputnik 1 necessitated a clarification as to the legal categorization of outer space for the purposes of international law. The 'starting point' of outer space was among the first issues put to UNCOPUOS for discussion, but, as noted, the question of where airspace 'ends' and outer space 'begins' has thus far remained unanswered from an international legal viewpoint.

The issue of the 'definition and delimitation of outer space' remains on the agenda of UNCOPUOS meetings,[239] and continues to give rise to divergent views among Member States as to where any such demarcation point might lie or, indeed, whether it is necessary at all to determine such a point.

Australia's legislative position

Australia was the sixth country in the world to introduce domestic space law - the *Space Activities Act 1998* (Cth).[240] This legislation was amended in 2002 by the *Space Activities Amendment Act 2002* (Cth), which sought to address the vexed question as to where space begins, albeit only for the purposes of the legislation. It was considered that the absence of a precise clarification of when and how the legislation would apply could conceivably lead to uncertainties as to which activities were to be regulated.

To address the issue for the purposes of the Space Activities Act, the legislation incorporated into the definitions of a 'launch', a 'launch vehicle', a 'return' and a 'space object' a reference to 'the distance of 100 [kilometres] above mean sea level'.[241] At the time of introducing this clearly defined point, the then Minister for Industry, Science and Resources explained that it was necessary to 'provide certainty to industry about the point where industry players become subject to the provisions' of the legislation, by addressing 'the issue that there is uncertainty as to where 'outer space' begins given that there is no definitive explanation of the term in either Australian or international law.'[242]

The Australian legislative framework for space activities was amended in 2018, and the relevant legislation is now called the *Space (Launches and Returns) Act 2018* (Cth). Whilst there have been some significant amendments to the original legislation, this element of the law has remained unchanged – i.e. the definition of 'launch', 'return' and 'space object' all retain a reference to 'area beyond the

[238] Ibid.
[239] See, United Nations Committee on the Peaceful Uses of Outer Space, *Report of the Legal Subcommittee on its 58th session, held in Vienna from 1 to 12 April 2019*, 58th sess, 58th mtg, UN Doc A/AC.105/ (31 May 2019).
[240] For background see Australian Government, 'Australia' (Submission to Space Debris Mitigation Standards, November 2013) <https://www.unoosa.org/documents/pdf/spacelaw/sd/Australia.pdf>.
[241] *Space Activities Act 1998* (Cth), s 8.
[242] Memorandum, *Space Activities Amendment Bill 2002 (Cth)* February 2002 4.

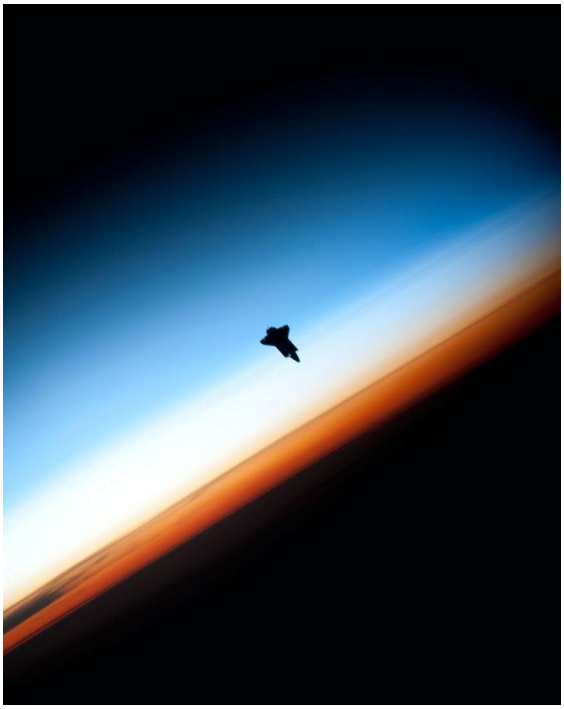
distance of 100 km above mean sea level'.[243]

There was also the question of the 'status' of outer space. Although the USSR had not sought the permission of other States to undertake the Sputnik 1 mission, there were no significant protests that it had infringed on any country's sovereignty as it circled the Earth. This international (in)action confirmed that, from the perspective of States, this new frontier of human activity did not possess the elements of sovereignty that had already been well established under the international law principles regulating land, sea and airspace. As was observed by Judge Manfred Lachs of the International Court of Justice:

> The first instruments that men sent into outer space traversed the airspace of States and circled above them in outer space, yet the launching States sought no permission, nor did the other States protest. This is how the freedom of movement into outer space, and in it, came to be established and recognised as law within a remarkably short period of time.[244]

However, notwithstanding the lack of a clear definition of outer space, a number of fundamental legal principles relating to the exploration and use of outer space emerged quite quickly following the Sputnik 1 mission, although their codification into a treaty form took more time. This was due to a number of reasons, including the unique environment with which any legally binding instrument would have to deal, the significant geopolitical and strategic factors at play, and the rapid growth of space-related technology that followed almost immediately from the Sputnik 1 success.

Thus, several foundational principles of the international law of outer space were born already by the early 1960s – in particular, the so-called 'common interest', 'freedom' and 'non-appropriation' principles. These were later incorporated into the terms of the UN Space Treaties,[245] with the result that they also constitute binding conventional rules, codifying what had already amounted to principles of customary international law.



As noted, these fundamental rules represent a significant departure from the legal rules relating to airspace,

---

[243] *Space (Launches and Returns) Act 2018* (Cth), s 8. A possible anomaly in Australia's legislative framework, and one that (arguably) may not be entirely consistent with the principles of the *Outer Space Treaty* noted above, lies in section 18 of the *Radiocommunications Act 1992* (Cth), which provides that:
'Application to the atmosphere etc.
Except so far as the contrary intention appears, references in this Act to Australia, a foreign country, a place or any waters include references to the space (including the atmosphere *and outer space*) above' (emphasis added).

[244] *North Sea Continental Shelf Cases (Federal Republic of Germany v. Denmark and Federal Republic of Germany v. The Netherlands)* (Judgment), Dissenting Opinion of Judge Lachs [1969] ICJ Rep 3, 230.

[245] *See*, for example, *Outer Space Treaty* (n 202) arts 1, 2.

which is categorized as constituting part of the 'territory' of the underlying State. The territorial nature of airspace is reflected in the principal air law treaties.[246] The International Court of Justice has confirmed that this characteristic of airspace also represents customary international law.[247]

As a consequence, civil and commercial aircraft have only certain limited rights to enter the airspace of another State,[248] in contrast to the freedom principle relating to outer space.[249] Even though, as noted above, the delimitation between airspace and outer space has not (yet) been definitively agreed, this has not in practice led to any significant confusion as to 'which law' might apply in particular circumstances.[250]

By contrast to the position regarding airspace, Article II of the Outer Space Treaty encompasses the 'non-appropriation' principle.[251] As noted above, the provision reads:

> Outer space, including the moon and other celestial bodies, is not subject to national appropriation by claim of sovereignty, by means of use or occupation, or by any other means.

In general terms, Article II confirms that outer space (which includes the Moon and other celestial bodies) is not subject to ownership rights and prohibits inter alia any sovereign or territorial claims to outer space. Outer space therefore is not to be regarded as 'territorial', a principle that was already well accepted in practice. Indeed, by the time that the Outer Space Treaty was finalized, both the United States and the USSR had been engaged in an extensive range of space activities; yet neither had made a claim to sovereignty over any part of outer space, including celestial bodies, notwithstanding the planting by the Apollo 11 astronauts of an American flag on the surface of the Moon,[252] or the much more recent placement of a Chinese flag on the

---

[246] For example, reaffirming the principle already acknowledged as early as in the *Convention on the Regulation of Aerial Navigation*, opened for signature 13 October 1919 11 LNTS 173 (entered into force 15 June 1929) (*Paris Convention*). See also, *Convention on International Civil Aviation*, opened for signature 7 December 1944, UNTS 15 102, (entered into force 4 April 1947), art. 1 ('*Chicago Convention*'), which provides that 'every State has complete and exclusive sovereignty over the airspace above its territory.'

[247] In *Nicaragua v United States of America* (n 147) 128, the court noted that '[t]he principle of respect for territorial sovereignty is also directly infringed by the unauthorized overflight of a State's territory by aircraft belonging to or under the control of the government of another State'.

[248] See *Chicago Convention* (n 246) arts 5, 6.

[249] Of course, any space activities requiring a launch from Earth and/or a return to Earth will also involve a 'use' of airspace. In this respect, the law of airspace may be relevant to the legal position if, for example, the space object of one State travels through the airspace of another State. See also *Liability Convention* (n 202), which applies *inter alia* to 'aircraft in flight' (*i.e.* in airspace).

[250] However, as the range of activities in outer space becomes ever broader, the issue will become more important in relation not only to the broad principles of international space law but also on a practical level – for example, to the regulation of commercial sub-orbital space tourism activities: see Steven Freeland, 'Fly Me to the Moon: How Will International Law Cope with Commercial Space Tourism?' (2010) 11:1 *Melbourne Journal of International Law* 90.

[251] For a detailed analysis of the *Outer Space Treaty* (n 201) art. II, see Steven Freeland and Ram Jakhu, 'Article II' in S. Hobe, B. Schmidt-Tedd and K.-U. Schrogl (eds.), *Cologne Commentary on Space Law, Volume I – Outer Space Treaty* (Carl Heymanns Verlag 2009) 44.

[252] This is to be compared with the situation in Antarctica, which had seen a series of sovereign claims by several States in the period leading up to the finalization in 1959 of The *Antarctic Treaty,* opened for signature 1 December 1959, 5778 UNTS 402 (entered into force 23 June 1961) ('*Antarctic Treaty*'). Article IV of the Antarctic Treaty has the effect of suspending all claims to territorial sovereignty in Antarctica for the duration of that instrument, as well as prohibiting any 'new claim, or enlargement of an existing claim'. The Protocol on Environmental Protection to the Antarctic Treaty, 30 I.L.M. 1455, which came into force in 1998, augments the Antarctic Treaty by protecting Antarctica from commercial mining for a period of 50 years: see Steven Freeland and Anja Pecujlic, 'How do you like your Regulation – Hard or Soft? The Antarctic Treaty and the Outer Space Treaty Compared' (2018) 30(1) *National Law School of India Review* 11.

Moon as part of that country's Chang'e 5 mission.[253]

The codification of this non-appropriation principle immediately follows Article I, which elaborates on the 'common interest' and 'freedom' principles and confirms that the exploration and use of outer space is to be undertaken 'for the benefit and in the interests of all countries' and freely 'by all States without discrimination of any kind, on a basis of equality and in accordance with international law'. In general terms, the primary intent of Article II was to reinforce these important concepts by confirming that principles of territorial sovereignty do not apply to outer space. Not only does this reflect the practice of States from virtually the beginning of the space age,[254] but it was an important proactive step designed to protect outer space from the possibility of conflict driven by territorial or colonizing ambitions.

In this regard, the United States delegate to UNCOPUOS at the time, Mr. Herbert Reis, reiterated the specific object and purpose of Article II on 31 July 1969, just a matter of days after the Apollo 11 astronauts had landed on the Moon, by stating as follows:

> The negotiating history of the Treaty shows that the purpose of this provision [Article II] was to prohibit a repetition of the race for the acquisition of national sovereignty over overseas territories that developed in the sixteenth, seventeenth, eighteenth and nineteenth centuries. The Treaty makes clear that no user of space may lay claim to, or seek to establish, national sovereignty over outer space. [255]

The sentiments reflected in Article II are therefore fundamental to the regulation of outer space and its exploration and use for peaceful purposes. A binding principle of non-appropriation is an essential element of international space law, to be preserved and followed in the conduct of all activities in outer space. Simply put, it

[253] Dustin Jones, 'Chinese Chang'e-5 Is Returning From Moon With Rocks, Left A Flag To Celebrate' *National Public Radio* (Article, 4 December 2020). <https://www.npr.org/2020/12/04/943292359/chinese-change-5-is-returning-from-moon-with-rocks-left-a-flag-to-celebrate>.

[254] One notable exception in this regard was the Bogota Declaration. In 1976, a number of equatorial States – including Brazil, Colombia, the Congo, Ecuador, Indonesia, Kenya, Uganda and Zaire – claimed sovereign rights over segments of the geostationary synchronous orbit above their respective territories, principally based upon the lack of an accepted delimitation between airspace and outer space. See also art. 101 of the Constitution of Colombia, which provides in part as follows, [*Constitución Política de Colombia 1991,* art. 101 tr: Constitute Project]:

> Also part of Colombia is the subsoil, the territorial sea, the contiguous zone, the continental shelf, the exclusive economic zone, the airspace, *the segment of the geostationary orbit, the electromagnetic spectrum and the space where it applies*, in accordance with international law or the laws of Colombia in the absence of international regulations (emphasis added).

[255] E.N. Valters, 'Perspectives in the Emerging Law of Satellite Communications' (1970) 53(5) *Stanford Journal of International Studies* 66.

is at the heart of how we view space, how we conduct activities in space and how we 'defend' space (including celestial bodies) from actions that will, in the end, threaten its viability as an area from which humanity can derive significant developments necessary for its future survival.

Sovereign rights in space

While no State has absolute sovereignty in space, they may, in certain circumstances, have sovereign rights in space. For example, as noted, much like the situation for flagged vessels on the high seas.[256] of for commercial aircraft,[257] States have sovereign rights to regulate their nationals and space objects.[258]

Sovereign rights over nationals and space objects

Article VI of the Outer Space Treaty specifies that the activities of non-government entities require authorization and supervision by the 'appropriate State'.[259] Article VIII of the Outer Space Treaty provides that '[a] State Party to the Treaty on whose registry an object launched into outer space is carried shall retain jurisdiction and control over such object, and over any personnel thereof ... [and that] [o]wnership of objects launched into outer space . . . is not affected by their presence in outer space . . . or by their

return to the Earth.'[260]

The provision can be interpreted as confirmation that the State of registry

KEY POINT:

"There is currently no agreement as to the precise delineation between outer space and airspace. Although in practical terms this has thus far not proven to pose major difficulties, it is an obstacle in clarifying the nature of sovereignty because of competing legal regimes: Earth-bound and space-bound; as well as the different national defence interests in both."

[256] *United Nations Convention on the Law of the Sea,* opened for signature 10 December 1982, 1833 UNTS 3 (entered into force 16 November 1993) art 89-90.
[257] *Chicago Convention* (n 246) art 17.
[258] For a more detailed discussion of this point, see Ireland-Piper and Freeland (n 215).
[259] *Outer Space Treaty* (n 202) art. VI.
[260] Ibid art VIII (emphasis added).

KEY POINT:

The effect of Article VIII of the Outer Space Treaty is that Australia retains ownership of objects it launches into space and that legal authority over that object and personnel remains.

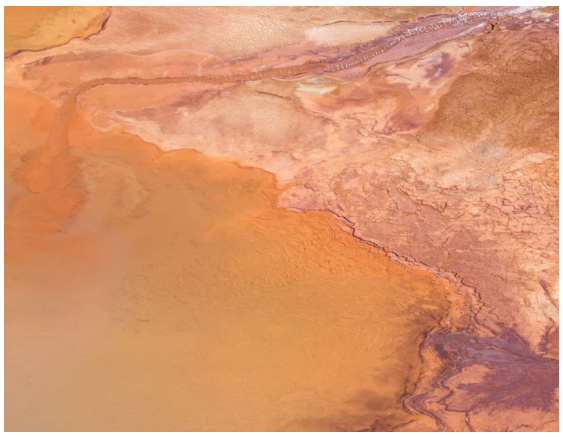
shall maintain jurisdiction over not only the space object, but also over any personnel on board the spacecraft, regardless of that person's nationality. As noted, this apportionment of control parallels the basic conventions of 'flagship' jurisdiction under international law of the sea.

As a practical matter, Article VIII's jurisdictional provision draws a distinction between criminal acts carried out onboard a spacecraft and criminal acts carried out outside any spacecraft or space object. Whilst this latter case may represent a regulatory 'gap', the legal position is that States retain some sovereign rights over their citizens and objects in outer space. This may also mean assuming responsibility or liability for wrongful acts undertaken by those citizens or caused by those objects, a conclusion that is reinforced by Articles VI and VII of the Outer Space Treaty, as well as the liability regime established for a 'launching State' under the Liability Convention.

Sovereign rights to natural resources

An issue that, if not appropriately governed, may give rise to future conflict is competition for natural resources in space, particularly in the context of 'space mining'. International law does recognise a – terrestrial – sovereign right to natural resources, which has long been accepted,[261] but the situation is not as clear with respect to space resources.

Recent developments might give rise to a perception that commercial off-Earth mining activities might soon be undertaken and that the prevailing



[261] *Permanent sovereignty over natural resources*, GA Res 1803 (XVII), UN GAOR, 28th sess, 2203rd plen mtg, UN Doc A/RES/3171 (17 December 1973). The principle of 'Permanent Sovereignty over Natural Resources' (PSONR) was established during the 1960s, and was initially focused on developing countries, although it was subsequently extended to include the rights of 'peoples' to regain effective control over their natural resources. There have been many United Nations General Assembly Resolutions relating to PSONR: see, for example, United Nations General Assembly Resolution 1803 (XVII) (14 December 1962) *Permanent sovereignty over natural resources*, GA Res 1803 (XVII), UN GAOR, 28th sess, 2203rd plen mtg, UN Doc A/RES/3171 (17 December 1973) and *Permanent sovereignty over natural resources of developing countries and expansion of domestic sources of accumulation for economic development,* GA Res 2692 (XXV), UN GAOR (11 December 1970). The PSONR has also been expressly incorporated into significant documents relating to the exploration and use of outer space: see, for example, *Remote Sensing Principles* (n 212), Principle IV of which provides inter alia that remote sensing activities 'shall be conducted on the basis of respect for the principle of full and permanent sovereignty of all States and peoples over their own wealth and natural resources'.

legal regime applicable to such activities is determined in accordance with national law. Whilst, of course, it is clear that national law is necessary in order to regulate the activities of private / non-governmental entities, off-Earth mining by those entities will still constitute 'national activities in space', for which States bear international responsibility under the existing international legal framework. Clearly, therefore, the international legal regime will be applicable to any such activities, particularly given the non-territorial *res communis* nature of outer space.

However, little is known about the potential impact of mining in space on the stability of both the space and Earth environments, particularly in relation to the impact the Moon has on tidal activity on Earth. In turn, this may cause conflict between States, including in the context of 'emerging rights to a clean and healthy environment'[262] of citizens and over questions of liability.

This is discussed further below in the context of defence implications.

Sovereign obligations in space

In addition to Australia having sovereign rights over its objects and personnel in outer space, Australia also has sovereign obligations in outer space.

Activities in outer space are to be carried out in accordance with international law. This means that Australia's international obligations as a sovereign State, including in relation to the conduct of armed hostilities, may continue to apply in space. By way of further example, there is no legal reason why the jurisdiction of the International Criminal Court (ICC) would not extend into outer space, although there may well be practical reasons relating to enforcement in terms of time and distance.[263] In any event, it would only apply, as it does on Earth, with respect to individual criminal responsibility for the crime of genocide, crimes against humanity, war crimes, and the crime of aggression.[264]

It would also only apply if the 'State on the territory of which the conduct in question occurred or, if the crime was committed on board a vessel or aircraft, the State of registration of that vessel or aircraft' was a State Party; or where, 'the State of which the person accused of the crime is a national' is a State Party.[265] Australia is a State party to Rome Statute of the International Criminal Court,[266] Article 1 of which provides that its jurisdiction 'shall be

[262] United Nations Educational, Scientific and Cultural Organisation, *Experts' Meeting on the Right to Enjoy the Benefits of Scientific Progress and its Applications* (Programme and Meeting Document, SHS/RSP/HRS-GED/2009/PI/H/1, 17 July 2009) 6 (*Experts' Meeting on Scientific Progress*).
[263] See, generally, Steven Freeland, 'International Criminal Justice in the Asia-Pacific Region: The Role of the International Criminal Court Regime' (2013) 11(5) *Journal of International Criminal Justice* 1029.
[264] *Rome Statute of the International Criminal Court,* opened for signature 17 July 1998, 2187 UNTS 90 (entered into force 1 July 2002) ('*Rome Statute*'), art. 5(1).
[265] *Rome Statute* (n 264) art 12.
[266] Ibid art 1.

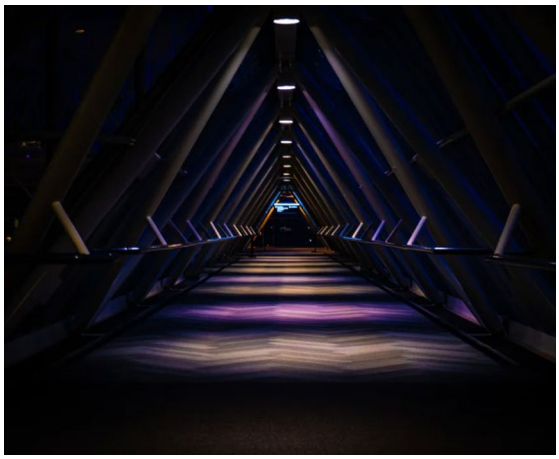
complementary to national criminal jurisdictions'. In the event that one of the four serious international crimes were to take place in outer space and the jurisdictional requirements were met, it is likely that the ICC could exercise jurisdiction (or an individual nation State could decide to exercise universal jurisdiction), although there may be practical challenges with respect to the gathering of appropriate evidence to support the existence of such a crime.

A State may owe legal obligations to persons who are not its citizens if such persons are under its 'effective' or 'overall' control.[267] In its 2004 advisory opinion, Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory (Wall Opinion),[268] the International Court of Justice held that a State party to the International Covenant on Civil and Political Rights[269] remains legally bound to comply with its provisions, even when exercising jurisdiction outside its national territory.[270] As a State party to that instrument, Australia's human rights obligations will follow it into outer space in circumstances where Australia is exercising effective control.

Defence implications of sovereignty in outer space

Weapons testing and development

Since the launch of Sputnik 1 in 1957, humankind has to a large degree respected the 'peaceful purposes' requirement that underpins the UN Space Treaties. We have not seen a space object destroyed in anger – although several States have deliberately destroyed their own satellites[271] – and space has not become



[267] For an explanation of the attribution of the State to conduct of non-citizens, see, Stefan Talmon, 'The Responsibility of Outside Powers for acts of Secessionist Entities' (2009) 58 *International and Comparative Law Quarterly* 493.

[268] *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory (Advisory Opinion)* [2004] ICJ Rep 136 ('*Wall Opinion*').

[269] *International Covenant on Civil and Political Rights*, opened for signature 19 December 1996, 999 UNTS 171 (entered into force 23 March 1976) ('*ICCPR*').

[270] Wall Opinion (n 268) 179. Israel was found to be bound by its obligations under *ICCPR* on the basis that it was exercising a type of territorial jurisdiction over Occupied Palestine; see, also, the decision of the European Court of Human Rights in the case of *Bankovic and Others v Belgium and Others* (European Court of Human Rights, Grand Chamber, Application No 52207/99, 12 December 2001). In that case, an application by six citizens of the Federal Republic of Yugoslavia asserted that the bombing of a radio and television building by North Atlantic Treaty Organisation ('*NATO*') during the Kosovo crisis in April 1999, in which a number of people were killed, violated the right to life in Article 2, and the freedom of expression in Article 10, of the European Convention on Human Rights. The Court declared the application inadmissible on the basis that there was no jurisdictional link between the victims of the act and the respondent States. For background to the bombing, see Steven Freeland 'The Bombing of Kosovo and the Milosevic Trial: Reflections on Some Legal Issues' (2002) *Australian International Law Journal* 150.

[271] As is well known, the latest of these 'tests' was conducted by India on 27 March 2019 – ironically three days before the start of the 58th session of the Legal Subcommittee of UNCOPUOS – when it deliberately destroyed by kinetic means an Indian satellite orbiting at approximately 285 kilometres above the Earth; see Marco Langbroek,

a theatre of warfare, notwithstanding more recent calls by some for it to be regarded as a 'war fighting domain', a generalised categorization that we believe should be resisted and rejected.[272]

From this perspective, space has actually 'worked' reasonably well, itself quite a remarkable feat of law and the rule of law, and its facilitation of responsible norms of behaviour, given the rapid development of (military) space technology over the past six decades. In this regard, space law has played a positive role, by allowing for – and not unduly restricting – the development of space-related technology and ensuing human rights benefits, whilst discouraging and proscribing bad behaviour, which would have negative consequences on the enjoyment of human rights.

For example, it is evident that the utilisation of space technology has allowed for significantly better access to information, communications, technology and infrastructure for less developed countries, a transformation that has been significantly enhanced through the establishment, in the 1970s, of INTELSAT, whose original purpose was to provide satellite services and infrastructure to such countries in a way that would promote higher standards of living and conditions of economic and social progress.[273]

At the same time, the existing legal regime has not prevented the development of military technology capable of utilizing outer space. Whilst there are some restrictions in the Outer Space Treaty, these were specified in relatively general terms and were open to divergent interpretation as to what they did (and did not) prohibit. This is not entirely surprising, given the time that the instrument was concluded, and that the development of space-related technology was, at least initially, inextricably related to military strength – both in reality and to influence the perception of others.

Since those early days, the situation has, if anything, become significantly more complex, with potentially drastic and catastrophic consequences, including for the enjoyment of human rights relating to life and safety. Just as the major space-faring nations have been undertaking what might be termed 'passive' military activities in outer space, outer space is increasingly now being used as part of active engagement in the conduct of armed conflict.[274] Not only is information

---

'Why India's ASAT Test was Reckless', *The Diplomat* (Web Page, 30 March 2019) <https://thediplomat.com/2019/05/why-indias-asat-test-was-reckless/>.

[272] See: Steven Freeland, 'The US Plan for a Space Force risks escalating a 'Space Arms Race' *The Conversation* (Web Page, 10 August 2018) <https://theconversation.com/the-us-plan-for-a-space-force-risks-escalating-a-space-arms-race-101368>.

[273] INTELSAT was created through a multilateral treaty with the desire to produce telecommunications "for the benefit of all [hu]mankind"; *Agreement relating to the International Telecommunications Satellite Organization "INTELSAT"*, opened for signature 20 August 1971, UNTS 1220 (entered into force 12 February 1973). The United States advocated at the United Nations for the establishment of the international organisation to provide a single global public telecommunications network. See: Bert Rein and Carl Frank, 'The Legal Commitment of the United States to the INTELSAT System' (1989) 14(2) *North Carolina Journal of International Law* 219. Alongside ambitions of social progress, INTELSAT provided high quality telecommunication that were economically viable through international collaboration of governments and private enterprise; F. G. Nixon, 'Intelsat: A Progress Report on the Move toward Definitive Agreements' (1970) 20(3) *The University of Toronto Law Journal* 380, 383. INTELSAT was privatised in 2001, and the International Telecommunications Satellite Organization ('ITSO') continues to fulfil its international obligations; ITSO, 'About Us' (Web Page, 2020) <https://itso.int/about-us/>.

[274] See, for example: Jackson Maogoto and Steven Freeland, 'The Final Frontier: The Laws of Armed Conflict and Space Warfare' (2007) 23(1) *Connecticut Journal of International Law* 165; David Simonds, 'A New Arms Race in Space?' *The Economist* (Web Page, 25 January 2007) 5 <https://www.economist.com/leaders/2007/01/25/a-new-arms-race-in-space>; Thomas E. Ricks, 'Space Is Playing Field for Newest War Game; Air Force Exercise

gathered from outer space – through, for example, the use of remote satellite technology and communications satellites – used to plan and undertake military engagement on Earth, but space assets are now also used to direct military activity and thus represent an integral part of the military hardware of the major powers.[275]

It is now within the realms of reality that outer space may itself become an emerging theatre of warfare. Designations of space as simply to be thought of as 'contested, congested and competitive',[276] with war in space described in some military circles as 'inevitable', are dangerously self-fulfilling and largely self-defeating: all States, particularly the major space-faring ones, will suffer if activities in space are undertaken in such an irresponsible manner as to cross certain 'red lines' of accepted behaviour.

Competition for natural resources

The solar system is replete with resources such as the water, minerals, precious metals found on moons and asteroids. This has attracted interest from both scientists and entrepreneurs.

Not only is this (potentially) of enormous financial value if transported back to Earth, but may also assist in onward space travel, and the building of future settlements and outposts. For example, in 2016, it was estimated that 711 known asteroids possess an estimated value exceeding $100 trillion.[277] One such asteroid, '16 Psyche,' is estimated to be worth over $10,000 quadrillion.[278] Technological equipment required for space mining, however, is still very much in its development phases. Nonetheless, in 2019, a collection of rock samples was taken from the asteroid Ryugu by Japanese spacecraft Hayabusa-2, which then returned to Earth in Australia.[279]

Shows Shift in Focus', *The Washington Post* (Web Page, 29 January 2001) A1 < https://www.washingtonpost.com/archive/politics/2001/01/29/space-is-playing-fieldfor-newest-war-game/938e9674-0c3b-4d66-b67b-e3195b1275fd/>.

[275] The current debate concerning Artificial Intelligence in outer space recognises the potential for violations of International Humanitarian Law due to its autonomy, which may infringe the principles of proportionality, distinction, precautions in attack. For an appraisal of current Artificial Intelligence concerns, see, Anne-Sophie Martin and Steven Freeland, 'The Advent of Artificial Intelligence in Space Activities: New Legal Challenges' (2021) 55 *Space Policy* 101408.

[276] See, for example: Government of Australia, *Working Paper by Australia to the UN Disarmament Commission 2018, 'Working Group on Transparency and Confidence Building Measures in Outer Space Activities'* Document A/CN.10/2018/WG.II/CRP.1 (28 March 2018) <https://www.un.org/disarmament/wp-content/uploads/2018/04/A-CN.10-2018-WG.2-CRP.11.pdf>.

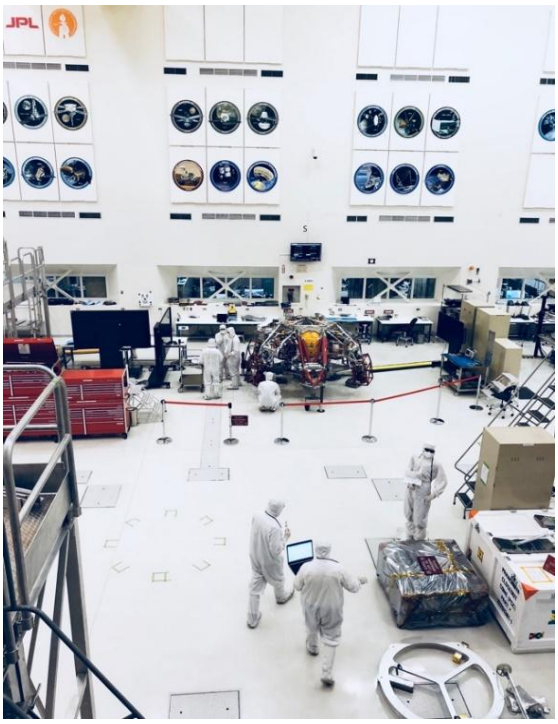
[277] Daniel Mikelson, *Intergalactic Travel and Asteroid Mining,* (Cambridge Stanford Books, 2019). For specific asteroids, see ASTERANK; Asterank, (Web Page) <http://www.asterank.com/>.

[278] Matthew Davis, *Will Asteroid Mining Be an Outer-Space Gold Rush?*, BIG THINK (Sept. 28, 2018) <https://bigthink.com/technology-innovation/economic-impact-of asteroidmining?rebelltitem=1#rebelltitem1> [https://perma.cc/NUQ9-ZRJC].

[279] This sample collection occurred approximately 300 million kilometres from Earth, with the return taking place at Woomera, Australia in December 2020. See Steven Freeland and Annie Handmer, 'Giant leap for corporations? The Trump administration wants to mine resources in space, but is it legal?', *The Conversation* (Web Page, 20 April 2020) <https://theconversation.com/giant-leap-for-corporations-the-trump-administration-wants-to-mine-resources-in-space-but-is-it-legal-136395> ('*Freeland and Handmer*').

Luxembourg, the United Arab Emirates (UAE), and the United States have indicated through their domestic laws an intention to facilitate and regulate space mining. Luxembourg passed legislation in 2017 'granting businesses operating within its jurisdiction rights in resources extracted in outer space'.[280] That legislation asserts 'space resources are capable of being appropriated in accordance with international law'.[281] In the UAE, Federal Law No. (12) of 2019 on the Regulation of The Space Sector,[282] expressly contemplates permits for the exploration, exploitation and use of space resources.[283]

In 2015, the US adopted the US Commercial Space Launch Competitiveness Act (H.R.2262)[284] to facilitate 'commercial exploration for and commercial recovery of space resources by United States citizens'.[285] However, the US approach distinguishes the term 'resources' from the term 'celestial bodies' used in Article II of the Outer Space Treaty. The US legislation prevents classification of spatial resources as a 'celestial body' and so rights are granted to the minerals in the celestial body, not the body itself. Essentially, according to this viewpoint, the US position is that the lawfulness of mining 'resources' in the celestial body, rather than



[280] Loi du 20 juillet 2017 sur l'exploration et l'utilisation des ressources de l'espace [Law of 20 July 2017 on the exploration and use of space resources] (Luxembourg) art. 1 [tr Vincent Wellens]. See also the discussion of Luxembourg's contentious space mining laws as compared with art. II of the *Outer Space Treaty* in Philip De Man, 'Luxembourg law on space resources rests on contentious relationship with international framework' (Working Paper No 189, Ku Leuven, Leuven Centre for Global Governance Studies, Institute for International Law, July 2017) 5.

[281] Stefan A. Kaiser, 'Legal Protection against Contamination from Space Resource Mining' (2017) 66(2) *German Journal of Air and Space Law* 282, 284 citing Luxembourg Space Law ('*Kaiser*').

[282] *Federal Law No. (12) of 2019 on the Regulation of The Space Sector* (United Arab Emirates) 19 December 2019, Corresponding to 22 Rabi' Al-Akhar 1441H [*Federal Law No. 12 of 2019*]. See also Kelsey Warner, 'UAE looks to regulate asteroid mining as it aims to lure private space sector' (Web Page, 26 November 2019) <https://www.thenational.ae/uae/science/uae-looks-to-regulate-asteroid-mining-as-it-aims-to-lure-private-space-sector-1.943028>; Sam Bridge 'New UAE Space Law to open doors to foreign investment' *Arabian Business Industries* (Web Page, 28 February 2020) <https://www.arabianbusiness.com/technology/441175-new-uae-space-law-to-open-doors-to-foreign-investment>.

[283] *Federal Law No. (12) of 2019 on the Regulation of The Space Sector* (United Arab Emirates) 19 December 2019, Corresponding to 22 Rabi' Al-Akhar 1441H [*Federal Law No. 12 of 2019*] art 18.

[284] *U.S. Commercial Space Launch Competitiveness Act*, 2 USC (2015).

[285] Interview with Steven Freeland, Professor of International Law at Western Sydney University (SpaceWatch.Global, SpaceWatch Asia Pacific, April 2020) (Steven Freeland Interview) referring to *U.S. Commercial Space Launch Competitiveness Act*, 2 USC (2015); Freeland and Handmer (n 278) citing *U.S. Commercial Space Launch Competitiveness Act*, 2 USC (2015); Stephan Hobe, 'The International Institute of Space Law adopts Position Paper on Space Resource Mining' (2016) 65(2) *German Journal of Air and Space Law* 204, 204 referring to *U.S. Commercial Space Launch Competitiveness Act*, 2 USC §402 (2015); see also discussion in Mariella Moon, 'Luxembourg's asteroid mining law takes effect August 1st', *Engadget* (Web Page, 30 July 2017) <https://www.engadget.com/2017-07-30-luxembourg-asteroid-mining-law-august-1.html>. See also Kaiser, (n 281) 282-286.

KEY POINT:

Luxembourg, the United States, and the United Arab Emirates have legislation expressly enabling mining of natural resources in space, albeit subject to international law obligations. Claims of a sovereign right to natural resources in space may have defence implications.

appropriating the celestial body itself, fills a gap in the Outer Space Treaty.[286] On this view, the 'use, ownership, possession and sale of mineral resources do not constitute a (national) appropriation by means of use or by any other means.'[287] The reality, however, is more nuanced and requires a more detailed multilateral understanding. It is pertinent to note also that it may arguably stand in contrast to the relevant terms of the Moon Agreement of 1979 (to which the US is not a State Party and therefore is not bound).[288] That treaty instrument provides:

> Neither the surface nor the subsurface of the moon, nor any part thereof or natural resources in place, shall become property of any State, international intergovernmental or non-governmental organization, national organization or non-governmental entity or of any natural person. The placement of personnel, space vehicles, equipment, facilities, stations and installations on or below the surface of the moon, including structures connected with its surface or subsurface, shall not create a right of ownership over the surface or the subsurface of the moon or any areas thereof. The foregoing provisions are without prejudice to the international regime referred to in paragraph 5 of this article.[289]

The Moon Agreement is only binding among only those 18 States who have ratified it.[290] Australia has signed the

[286] Kaiser (n 281) 283 referring to *U.S. Commercial Space Launch Competitiveness Act*, 2 USC (2015) (n 284) and *Outer Space Treaty* (n 202); see generally Steven Freeland and Ram Jakhu, 'What's human rights got to do with outer space? Everything!' in R. Moro-Aguilar, P.J. Blount and T. Masson-Zwaan (eds), *Proceedings of the International Institute of Space Law 2014* (Eleven International, 2014) 365, 369 ('*Freeland and Jakhu*').
[287] Kaiser (n 281) 283-4.
[288] Ibid, 284-285 citing *Moon Agreement* (n 206).
[289] *Moon Agreement* (n 206) art 11.3.
[290] *Moon Agreement* (n 206). The Moon Agreement has to date been ratified by Armenia, Australia, Austria, Belgium, Chile, Kazakhstan, Kuwait, Lebanon, Mexico, Morocco, Netherlands, Pakistan, Peru, Philippines, Saudi Arabia, Turkey, Uruguay and Venezuela whilst France, Guatemala, India and Romania, are signatories: See, United Nations Office for Outer Space Affairs, 'Status of International Agreements Relating to Activities in Outer Space as at 1 January 2020' (1 January 2020) < https://www.unoosa.org/documents/pdf/spacelaw/treatystatus/TreatiesStatus-2020E.pdf >; United Nations

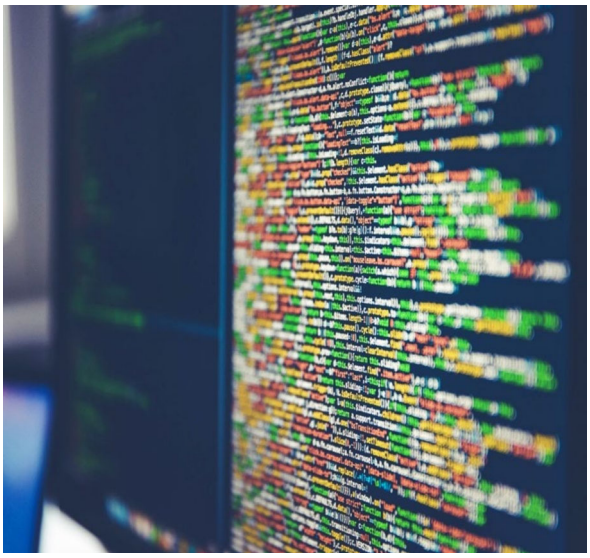
Moon Agreement. More recently, NASA and several partner countries (Australia, Canada, Italy, Japan, Luxembourg, United Arab Emirates, United Kingdom, and the United States of America) have signed 'The Artemis Accords', which establish principles 'to guide space exploration cooperation among nations participating in the agency's 21st century lunar exploration plans'.[291] The Artemis Accords are stated as reinforcing the Outer Space Treaty, the Registration Convention and 'other norms of behaviour that NASA and its partners have supported, including the public release of scientific data'.[292]

Information and intelligence gathering

Remote sensing is conducted via satellites and aircraft that detect and record imagery.[293] Some satellite images are commercially available, with such images 'becoming sharper and taken more frequently'.[294] In 2008, there were 150 Earth observation satellites in orbit; by June 2019, there were 768.[295] These numbers are set to increase even more dramatically with the advent of proposed large constellations of small Earth observation satellites.

The term 'remote sensing of the Earth from outer space' was defined in the 1979 Convention on the Transfer and Use of Data of Remote Sensing of the Earth from Outer Space as:

> observations and measurements of energy and polarization characteristics of self-radiation and reflected radiation of elements of the land, ocean and atmosphere of the Earth in different ranges of electromagnetic waves which facilitate the location, description of the nature and temporal variations of natural parameters and phenomena, natural resources of the Earth, the environment as well as anthropogenic objects and formations.[296]



In turn, the Principles relating to Remote Sensing of the Earth from Outer Space describe remote sensing as:

> making use of the properties of electromagnetic waves emitted,

---

Committee on the Peaceful Uses of Outer Space, *Report of the Committee on the Peaceful Uses of Outer Space,* 62nd sess, UN Doc A/74/20 (20 August 2019).

[291] NASA, 'International Partners Advance Cooperation with First Signings of Artemis Accords' (Press Release, 14 October 2020) <https://www.nasa.gov/press-release/nasa-international-partners-advance-cooperation-with-first-signings-of-artemis-accords>.

[292] Ibid.

[293] National Aeronautics and Space Administration, 'What is Remote Sensing', *Earthdata* (Web Page) <https://earthdata.nasa.gov/learn/remote-sensing>.

[294] Christopher Beam, 'Soon, satellites will be able to watch you everywhere all the time: Can privacy survive?' *MIT Technology Review* (Web Page, 26 June 2019) <https://www.technologyreview.com/2019/06/26/102931/satellites-threaten-privacy/>.

[295] Ibid.

[296] *Convention on the Transfer and Use of Data of Remote Sensing of the Earth from Outer Space*, opened for signature 19 May 1978, ILM, (entered into force 21 August 1979).

reflected or diffracted by the sensed objects, for the purpose of improving natural resources management, land use and the protection of the environment.[297]

Remote-sensing technologies in outer space do have humanitarian applications. However, such technologies (and the data collected) also can be used to achieve national security and defensive objectives. Notably, Artificial Intelligence (AI) technology is an increasingly important element of space technology. Various aspects of AI potentially seem well suited to a number of current and proposed space applications, including the following:

(i) Remote sensing and monitoring for a broad array of missions, including environmental change, national security and aircraft and maritime tracking;

(ii) Communications between ground and space, and from satellite-to-satellite (particularly in the case of mega/large constellations of small satellites), using radio frequencies, optical-laser communications, radar and other technologies;

(iii) Data analytics, including policy and regulatory issues inherent in collecting massive amounts of information, and how that information can be used, as well as data privacy;

(iv) Satellites as an alternative to terrestrial-based systems, including cloud computing, cross-border broadband services, and other methods of data and information transfer.

The implementation of AI impacts upon privacy and security, including Australia's privacy and security. This is particularly so given that space has become a significant global 'economy',[298] with a multitude of private and commercial activities engaging in myriad space activities, each directed towards profitability without, one might speculate, sufficient thought being given to the (potential) defence and national security consequences.

[297] *Remote Sensing Principles* (n 211) principle I.

[298] The global space economy in 2020 has transitioned toward the private sector, with a decreased reliance on government spending; KPMG, *30 Voices on 2030: The future of space* (Report, May 2020) 25. The COVID-19 pandemic did not significantly impact the space sector with increase in the European space workforce and similar trends of successful launched, with growth of $9 billion USD reported, increasing the overall global space economy to $423.8 billion USD; Space Foundation, 'Global Space Economy Grows in 2019 to $423.8 Billion, The Space Report 2020 Q2 Analysis Shows' (Web Page, 30 July 2020) <https://www.spacefoundation.org/2020/07/30/global-space-economy-grows-in-2019-to-423-8-billion-the-space-report-2020-q2-analysis-shows/>.

Conclusion: A strategic role for Australia in space

There is no doubt that the use of space, and how space is 'viewed' has changed dramatically over recent years given the advent of technological development. This has opened up possibilities for an ever-broadening array of space activities by an increasing number of sovereign and non-State actors, and the inevitable further enhancement of space as a dual-use area. The existing regulatory regime has largely served us well and, in many respects, has been remarkably successful. But the 'spacescape' is changing very quickly, driven by this bewildering technological maelstrom that, over the last five years or so (and certainly for the next period of time), has far surpassed the already rapid evolution in space-related technology that began at the beginning of the space race.

With these developments comes a greater dependence on continuous and unimpeded access to space for all countries, in particular for major industrialised powers with sophisticated military and national security infrastructures to protect and operate.

Those pressures somehow tend to assume a greater 'sovereign' interest in space, notwithstanding its non-territorial nature. One can foresee pressures in these two seemingly conflicting tensions.

Whatever the result, there will be a need for good 'international citizens' like Australia to play an increasingly significant strategic role in the discussions, negotiations and developments directed towards the safety, security and sustainability of space. The need for a more comprehensive and detailed legal/regulatory framework for outer space to meet these imperatives represents one of the most politicized and complex challenges ahead for our, and future generations. All stakeholders need to work together to find a path forward, in order to meet the challenges. The existing international regulatory framework, whilst important, cannot alone stand up to the complexities that the ever-increasing range of space activities – and the possibilities that still lie before us - impose.

CHAPTER

5

Concluding remarks

Concluding remarks

This Report has sought to bring increased clarity on the operation of the concept of sovereignty in the defence context. More specifically, it has sought to do so with a focus on the two domains of cyberspace and outer space.

The relevance of this topic was obvious already prior to the project's commencement. However, there is no doubt that it has increased further throughout the project. For example, the 2020 Strategic Update and the 2020 Force Structure Plan identified the management of cyber and information, and space, capabilities as strategically important, alongside maritime, air, and land capabilities.

The cyber and the space domains both have significant defence implications in their own right. Importantly, however, they are also crucial components of capabilities within the more traditional domains of maritime, air, and land. Put simply, the efficiency and strength of Australia's defence capabilities in the maritime, air, and land domains are directly dependent on capabilities in the cyber and the space domains.

Discussions of sovereignty now feature prominently in the defence context, as well as in the context of Australia's present day international relations. It is increasingly obvious that the definitions and delineations of key concepts such as 'sovereignty' is of great strategic importance. Consequently, if we were to single out one Recommendation as being more important than all others in this Report, it would be that Australia must work with its partners and allies to steer the direction of definitions and delineations in international law, including in relation to the centrally important concept of sovereignty. A pragmatic but principled approach to sovereignty will best serve Australia's strategic interests in contested areas like cyberspace and outer space.

Both cyberspace and outer space are dual use environments with both State and non-State actors present and both military and civilian applications. But while cyberspace is predominantly regulated by general international law, activities in outer space are subject to important international agreements.

Despite Article IV of the Outer Space Treaty making clear that '[t]he Moon and other celestial bodies shall be used by all States Parties to the [Outer Space] Treaty exclusively for peaceful purposes', the current (geo)political momentum appears to be directed towards an even greater incorporation of satellite technology in outer space as an integral part of the conduct of warfare. The way the concept of sovereignty develops in this context will be of great significance.

For the space domain, the twin policy for Australia of ensuring access to space through our strategic alliances with certain space-faring nations, whilst also developing further sovereign space capability in specific areas, is essential to Australian national security.

For the cyber domain, Australia needs to continue developing both its defensive and offensive capabilities. Given how interlinked civilian and military assets are in cyberspace, this must be done adopting a 'total defence' ('whole-of-society') approach under which civilian and military assets work together against cyber-attacks on Australian interests.

Concepts including 'data sovereignty' and 'technological sovereignty' are emerging, and the exact role of sovereignty is in debate in multiple forums simultaneously. Thus, what we are advocating is a broad and multifaceted engagement with current formative debates about the concept of sovereignty and its related concepts.

Such engagement is both an important component, and a facilitator, of Australia's commitment to a rules-based international order. Furthermore, uncertainty about the thresholds for activities that could trigger a military response in space or cyberspace undermines predictability and Australia's ability to respond to potential infringements of national interests in these domains, thus undermining Australia's capacity to defend its interests and those of its allies.

In parallel to the mentioned need for international norm-setting within the commitment to a rules-based international order, Australia must work on formulating a coherent understanding of sovereignty in the context of the space and cyberspace domains for its own purposes. This Report is just a starting point.

Any domestic formulation of a coherent understanding of sovereignty in the context of the space and cyber domains will need to be aligned with international developments on an ongoing basis. However, Australia cannot wait for international consensus to be formed. A domestic Australian formulation, for internal purposes, has become an even more pressing matter in the light of increasingly public ambitions to develop offensive cyberspace capabilities.

Looking towards the future there are at least two obvious directions for future research building on the work of this Report:

- The interaction and relationship between cyber and outer space – While the Report has highlighted both similarities and differences between the cyber environment and outer space, a natural next step is to explore the interaction and relationship between cyber and outer space. Most obviously, the cyber environment depends, in no small part, on satellites. Further, virtually all activity in outer space depends on a functioning cyber environment. Thus, disruptions – such as a cyber-attack or the sabotage of satellites – in one domain will directly impact the other domain, and Australia's defensive capabilities more broadly.

- The roles of cyber and outer space in hybrid 'grey zone' conflicts – Whilst debate will continue as to the characteristics of future war, the fact remains that in cyberspace and outer space, hostile acts are not the exclusive remit of nation States because the prevalence of modern information and communications technologies, and space technologies, has resulted in individuals having access to resources that can affect State interests. The other side of the proverbial coin is that foreign States may direct their cyber capabilities to severely disrupt Australian society and undermine Australia's defensive capabilities by attacking civilian targets.

We hope to address these questions in future work.

The Developing Concept of Sovereignty

Dan Jerker B. Svantesson
Rebecca Azzopardi
Wendy Bonython
Jonathan Crowe
Steven Freeland
Samuli Haataja
Danielle Ireland-Piper
Nathan Mark