12-3-2012

The Regulation of Space and Cyberspace: One Coin, Two Sides

Brett Biddington
Edith Cowan University

DOI: 10.4225/75/57a84295befb0
13th Australian Information Warfare and Security Conference, Novotel Langley Hotel, Perth, Western Australia, 3rd-5th December, 2012

THE REGULATION OF SPACE AND CYBERSPACE: ONE COIN, TWO SIDES

Brett Biddington
Adjunct Professor, SRI -Security Research Institute, Edith Cowan University
Perth, Western Australia
bbidding@tpg.com.au

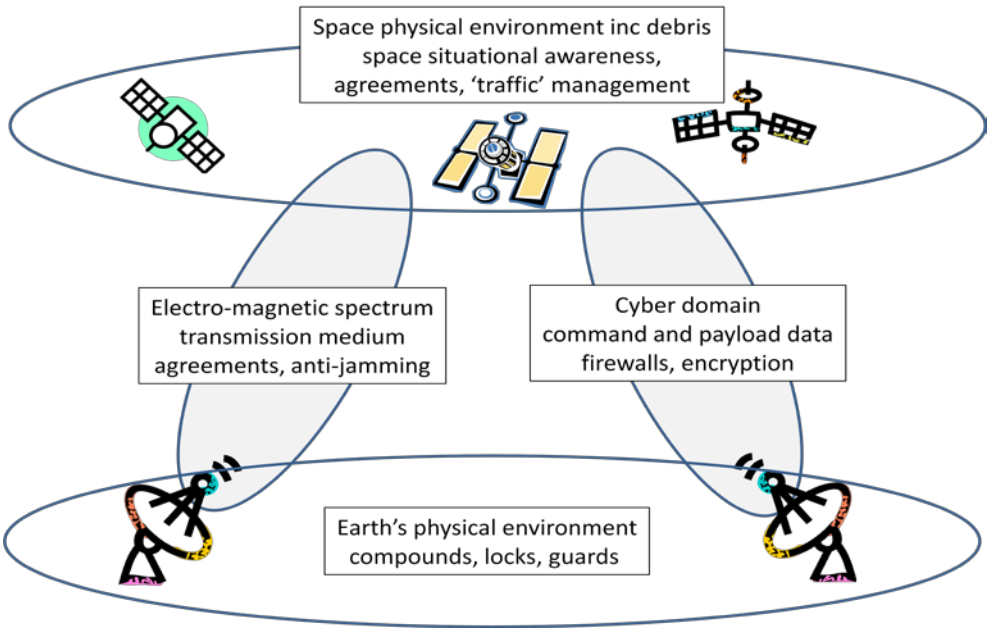
Abstract

In the 1960s, during some very tense days in the Cold War the United States of America (USA) and the Union of Socialist Soviet Republics (USSR) brokered a deal in the United Nations for a treaty regime to govern human activities in outer space. This regime has served well enough for almost 50 years. In recent years, however, fears of space weaponisation, the proliferation of space debris in the Low Earth Orbits (LEO) and increasing demands on the electromagnetic spectrum (EMS) have led to demands for regulatory reform. Some nations now consider space to be the fourth domain of modern warfare.

Meanwhile, the cyber domain continues to develop apace. The world is struggling to determine whether, and if so how, to regulate the cyberspace. The United States now considers cyberspace to be the fifth domain of warfare and has announced that it reserves the right to meet cyber attacks, on interests it considers vital, with conventional kinetic responses.

The space and cyberspace domains overlap and have mutual dependencies which demand a degree of coherence and integration in legislative, policy, and regulatory responses. There are also some important differences and distinctions. This paper explores some of the dilemmas that are faced by decision-makers who seek to make both the space and cyberspace domains safe and secure places which will deliver benefit to humans across the planet long into the future.

Keywords
Confidence building, cyberspace, dual use technology, security, space.



Protecting the Space Domain: A Multi-Dimensional Challenge
(Biddington & Sach, 2010)

SETTING THE SCENE

Human activity in space and the creation of cyberspace are broadly parallel developments in humanity's journey. Rockets and the development of computing, although with antecedents before World War II, leapt ahead during the war. The Germans developed the V2 rocket and the United Kingdom and the United States developed computers that were capable of breaking German and Japanese codes and ciphers.

The invention of the transistor in the 1940s, followed by the integrated circuit in the 1960s were fundamental enabling technologies for both space and cyberspace. The discipline of systems engineering was the organisational and methodological response which allowed the possibilities created by the transistor and the integrated circuit to be realised. Systems engineering emerged from Project Apollo, the US space program that put men on the moon.

These inventions caused a fundamental change in the way innovation occurs. Until the 1960s relatively clear distinctions could be drawn between inventions of military significance and those with broader application. In the 1960s the distinctions became less clear. Technologies and products that were developed to meet the demands of non-military markets were increasingly adopted and adapted by the military for warfighting. This comment applies especially to sensing technologies, analogue and digital signal processing, automated control systems and, more recently artificial intelligence, robotics and miniaturisation. Quickly these became known as 'dual use' technologies and they have been the subject of considerable argument ever since as regulators have sought to determine what does and does not constitute military technology and know-how of military value. More is said about the 'dual use' dilemma later in this paper and in a coda as well.

Regulating Space

Space activities have always been dominated by the activities of nation states. Initially there were two, the United States and the Union of Socialist Soviet Republics (USSR) now Russia. Now there are at least 12, including China, India and Japan. Although companies such as SpaceX are seeking to develop commercial, business to business space markets, their principal customer today and for the immediate future is the United States Government. In effect that government is transferring more technical and operational risk to SpaceX in an effort to reduce costs.[i]

In October 1962, President Kennedy of the United States and President Khrushchev, the leader of the Union of the Soviet Socialist Republics (USSR) now Russia, became embroiled in a game of chicken that brought the world to the brink of nuclear war. This was the Cuban missile crisis, where Russia, then lacking an Inter-Continental Ballistic Missile (ICBM) capability, sought to place Intermediate Range Ballistic Missiles (IRBM) on Cuba in order to directly threaten the United States. President Kennedy reacted by ordering a naval blockade of Cuba to prevent further missiles from being delivered to the island. Eventually, President Khrushchev blinked, ships carrying missiles from Russia turned back, the missiles already in place were dismantled and war was averted (Allison, 1971).

There are four points to note:

- From the beginning of the Cold War, which began more or less as soon as World War II ended, nuclear weapons and their delivery vehicles, missiles that fly through space, were inextricably linked in the minds of politicians, soldiers and diplomats.
- The Cuba missile crisis escalated very quickly, both sides understood the implications of miscalculation and shortly after the crisis ended set up a hotline between Washington and Moscow as one measure to avert nuclear war in the event of an accident that could appear as an attack.
- Both sides had good information about the military capabilities of the other but neither side had good understanding of the other's intent.
- The space programs (classified and unclassified) of both sides were in full swing.

The intense Cold War competition of the 1960s, exemplified by the Cuban missile crisis did not prevent the protagonists from working assiduously to put in place a regulatory regime for space that suited their own interests. This regime endures, although it is now under stress.

The *Outer Space Treaty* entered into force in 1967. It is the first of five treaties, four of which have been widely adopted, which guide the behaviour of nations in space. The Treaty outlines the following key concepts:

- the exploration and use of outer space shall be carried out for the benefit and in the interests of all countries and shall be the province of all mankind;
- outer space shall be free for exploration and use by all States;

- outer space is not subject to national appropriation by claim of sovereignty, by means of use or occupation, or by any other means;
- States shall not place nuclear weapons or other weapons of mass destruction in orbit or on celestial bodies or station them in outer space in any other manner;
- the Moon and other celestial bodies shall be used exclusively for peaceful purposes;
- astronauts shall be regarded as the envoys of mankind;
- States shall be responsible for national space activities whether carried out by governmental or non-governmental entities;
- States shall be liable for damage caused by their space objects; and
- States shall avoid harmful contamination of space and celestial bodies.[ii]

Especially relevant in the context of this paper are the concepts of benefit to all mankind, peaceful purposes and liability (which implies ownership and attribution).

The formal titles of the five treaties, together with information about their entry into force, ratifications and signatories follow.

- The Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies (the "Outer Space Treaty", adopted by the General Assembly in its resolution 2222 (XXI)), opened for signature on 27 January 1967, entered into force on 10 October 1967, 101 ratifications and 26 signatures (as of 1 January 2011);
- The Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space (the "Rescue Agreement", adopted by the General Assembly in its resolution 2345 (XXII)), opened for signature on 22 April 1968, entered into force on 3 December 1968, 91 ratifications, 24 signatures, and 1 acceptance of rights and obligations (as of 1 January 2011);
- The Convention on International Liability for Damage Caused by Space Objects (the "Liability Convention", adopted by the General Assembly in its resolution 2777 (XXVI)), opened for signature on 29 March 1972, entered into force on 1 September 1972, 88 ratifications, 23 signatures, and 3 acceptances of rights and obligations (as of 1 January 2011);
- The Convention on Registration of Objects Launched into Outer Space (the "Registration Convention", adopted by the General Assembly in its resolution 3235 (XXIX)), opened for signature on 14 January 1975, entered into force on 15 September 1976, 56 ratifications, 4 signatures, and 2 acceptances of rights and obligations (as of 1 January 2011);
- The Agreement Governing the Activities of States on the Moon and Other Celestial Bodies (the "Moon Agreement", adopted by the General Assembly in its resolution 34/68), opened for signature on 18 December 1979, entered into force on 11 July 1984, 13 ratifications and 4 signatures (as of 1 January 2011).[iii]

This is a slender body of international law to which can be added other multi-lateral agreements which seek to limit nuclear weapon and missile proliferation. These include:

- The Treaty banning Nuclear Weapon Tests in the Atmosphere, in Outer Space and Under Water (1963); and
- The Treaty on the Non-Proliferation of Nuclear Weapons (1973).
- The Missile Technology Control Regime (MTCR) established in 1987. This is an informal and voluntary association of countries which share the goals of non-proliferation of unmanned delivery systems capable of delivering weapons of mass destruction, and which seek to coordinate national export licensing efforts aimed at preventing their proliferation.

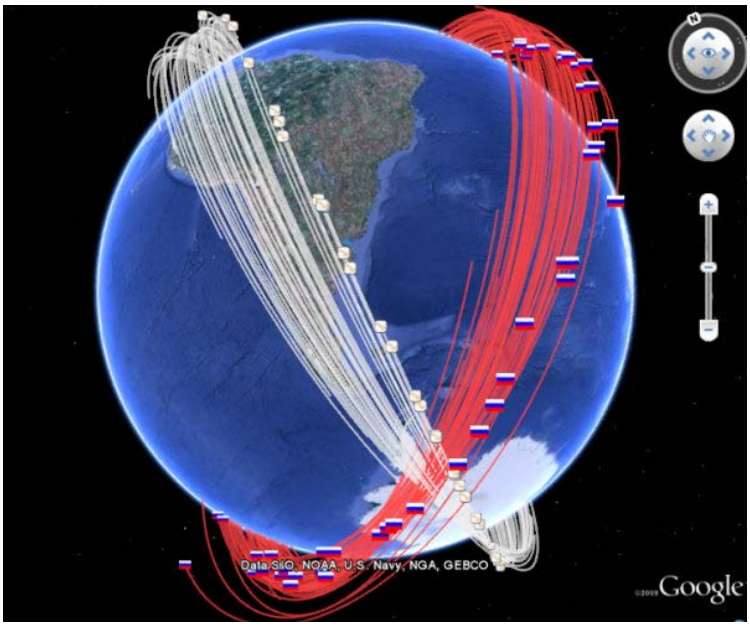
Within the United Nations there are two committees which consider matters concerning conduct in space. These are the Committee on the Peaceful Uses of Outer Space (COPUOS), based in Vienna and the Committee on Disarmament (CD) based in Geneva.

This regulatory regime worked well enough for 30-35 years. In the early 2000s, however, the situation began to change. The Rumsfeld Commission, formally the *Commission to Assess United States National Security Space Management and Organization*, submitted its report to Congress in January 2001. The report warned that the United States was considerably more dependent on space systems than any other nation and that to, '. . avoid a

"Space Pearl Harbor" it needs to take seriously the possibility of an attack on U.S. space systems.' (Rumsfeld, 2001, pp viii-ix)

Other nations were investing in space systems of their own and space was becoming increasingly "congested, contested and competitive".[iv] This phrase has now entered the lexicon and refers to three trends all of which are combining to force the world to re-think space regulation, and governance.

- The space environment, especially in the highly inclined Low Earth Orbits (LEO) is becoming increasingly congested. Space debris is an increasing problem and has led already to one collision between an operational US communications satellite (Iridium 33) and a defunct Russian communications satellite (Cosmos 2251). This collision, occurred in February 2009 over Siberia and created even more debris thus exacerbating the problem.[v]



Simulation Graphic of Iridium/Cosmos debris fields following collision over Siberia on 10 Feb 2009 [vi]

- The world of ubiquitous mobility is placing increasing pressure on parts of the electro-magnetic spectrum that are presently allocated to support space activities. There are two types of spectral bands that are essential to satellite operations. The first set are the frequencies used to pass command and control signals and data between ground control stations on Earth and satellites. The second set are the frequencies that are referred to by some as the "fingerprints of nature". These are the frequencies (absorption and reflectance spectra) that need to be kept clear in order that clouds, sea surface temperatures, floods, fires, forest growth, soil moisture and many other phenomena can be monitored from space.
- The number of space faring nations is increasing and their plans are becoming more ambitious and are not necessarily coincident. Not only do they need to cooperate to some agreed extent if space is to remain secure and accessible to all but the space disadvantaged nations (those nations which rely on the data and services provided by others from space) also have strong vested interests in ensuring that the space environment is well-managed into the future. Whereas in the 1960s, space was the private preserve of the United States and the USSR, today there are at least 12 nations which are capable of or on the cusp of being able to build, launch and operate satellites from their own territory. These include, in alphabetical order, Brazil, Canada, China, France, India, Israel, Japan, Russia, South Korea, Taiwan, the United Kingdom and the United States. Several other nations have developed IRBMs including Iran, North Korea and Pakistan. Another group of nations operate satellites which have been built and launched by others. Australia, Indonesia, Thailand, Vietnam and Nigeria are examples.

Space remains today, and is likely to remain for the foreseeable future, the preserve of a small number of nation states. It still represents the high ground for diplomacy and secure and assured access to space systems is absolutely essential for the conduct of military operations on Earth. Satellites allow nations to look into each other's back yards legally to gather intelligence as well as for treaty monitoring and verification purposes. The principal spacefaring nations are considered likely to tolerate commercial activities, such as those being developed by SpaceX, as well as incidental activities such as the space tourism business being developed by Virgin Galactic[vii] only so long as they do not interfere with vital national interests.

Nobody's interests are served if the space environment becomes so polluted with space debris that the risk of a collision between any working satellite and another object approaches certainty. There is also the question of radio frequency interference (RFI) whether unintentional or caused deliberately. Satellite operators are already fighting national governments as well as international organisations through the International Telecommunication Union (ITU) to preserve the spectrum needed to support communications between the Earth and satellites and between satellites themselves. A tipping point can be envisaged where governments and other would be investors in space systems may well walk away.

International activity which aims to make outer space a safer place is taking two basic forms. First is activity that has been in train for many years through the Committee on Disarmament. Called Prevention of an Arms Race in Outer Space (PAROS), the process aims to strengthen existing international space law with a new treaty. Russia and China are the main proponents of this approach.[viii] Second is activity initiated by the European Union to develop a space Code of Conduct.[ix] This is a less formal mechanism than a treaty and seeks to create norms or behaviours which nations will agree to follow voluntarily The aim is to stabilise the space environment especially by reducing the rate of growth of debris and by moving eventually to the adoption of debris reduction techniques.

Difficulties with the Code of Conduct approach include:

- Any Code will be voluntary and ultimately non-enforceable. Moral persuasion and the risk of international opprobrium for violating the Code are all that the international community can rely on to encourage compliant behavior.
- Space faring nations will need to agree about who owns what in space, including any debris that may be targeted for removal. This implies the creation, in the first instance of detailed, shared space situational awareness (SSA). Presently the United States has the most comprehensive SSA network of any nation. However, it takes great care to protect the actual operating parameters, strengths and limitations, of the system. Nations including China, are likely to insist on learning a great deal more about the United States SSA system before being will to accept its results and to act on them.
- Debris removal will be a delicate matter. A space garbage truck for one nation may appear to be a space weapon to another. Considerable confidence will need to be built between space faring nations before they are likely to agree to the removal of their property or that of a third party from space.

Since 2009 Australia has shown renewed interest in international space regulation. It is poised to release a national space policy early in 2013, has strengthened its commitment to SSA and is taking a more direct and active role in COPUOS than has been the case since the 1970s. The Australian Government now accepts the dependencies and associate vulnerabilities that many sectors of the Australian economy have on satellite systems.

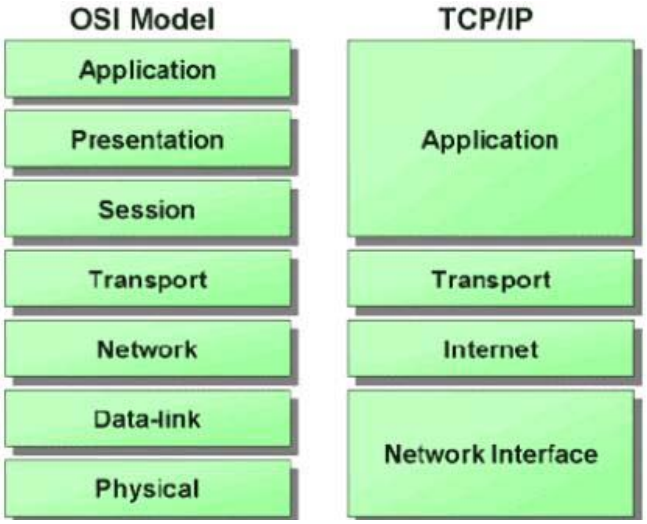
Regulating Cyberspace

This paper assumes that cyberspace is an environment in which activities may occur independently, if necessary, from activities in other domains. Certainly the United States is now referring to cyberspace as the fifth domain of warfare (after the sea, the land, the air and space) and it is no accident that the United States Air Force (USAF) links space and cyber security and deals with both in a single command.[x] [xi]

Unlike space, which is a natural environment that existed long before humans walked on Earth, cyberspace is an artificial environment that has been created by humans in the last fifty years. Whereas space is really difficult to access cyberspace is easy to access and becoming easier as the domain, considered as a system of systems, begins to behave as an ecosystem in which all parts are linked and the behavior of one influences, even ever so slightly, the behavior of every other. Less than 550 men and women have flown in space, today in the order of two and a half billion people, more than one third of the world's population, access the internet and the rate of connection continues to increase.[xii]

From the perspective of a person sitting at a computer terminal or linked to the internet through a mobile device, cyberspace is pervasive – everywhere and nowhere.

Whereas space is governed by a mix of international treaties, domestic laws and a number of international organisations, cyberspace hosts the internet which has become a global utility that is simply taken for granted by those who use it. Whereas the laws of physics are sufficient to describe the natural environment they are insufficient to describe cyberspace. The laws of physics still apply but the logic and underlying engineering of cyberspace also needs to be understood at least by those who shape the system. This structure is described, in general terms, in the diagram below which relates TCP/IP (Transmission Control Protocol/Internet Protocol), the foundation of the internet to the Open System Interconnection (OSI) model which shows the essential components of any network.



Source: ciscoiseasy.blogspot.com

The absolute and unambiguous nature of the binary mathematics which support the electrical and mechanical properties of transistors on integrated circuits leads to some very difficult questions about security and assurance and, more broadly, about regulation.

There are no specific international treaties or other international instruments that regulate or govern cyberspace. Behaviour in the domain is basically regulated by the domestic laws of the countries which touch cyberspace and that is all of the 200 or so nations on Earth. Criminal activity, major and minor, is routine. Offences against people, such as pedophiles grooming children, and offences against property, such as organised criminal gangs laundering money and committing scams and frauds, occur with mind-numbing frequency. Terrorists are known to use social media to recruit new members to their organisations and nation states are suspected of stealing data from other nations as well as from commercial entities of interest. Perhaps most seriously, some nation states are suspected of attempting to cause physical damage to particular facilities by extremely precise attacks against equipment control systems.

Cyberspace, because of the way in which it has evolved has two fundamental security weaknesses, neither of which would seem to have any easy or ready answer.

Some Comparisons and Contrasts

Both space and cyberspace are global commons. (Jasper, 2012) Both environments are fragile and easily disturbed physically and electro-magnetically. If severely damaged or degraded both environments could take a long time to restore, hundreds of years in the case of space. Space is largely the preserve of nation states with a well-defined, if outdated set of regulatory mechanisms, In contrast, cyberspace is used by a myriad of state and non-state actors and individuals for all manner of legitimate and illegitimate activities. Cyberspace is regulated by and large through existing legal mechanisms which are being adapted, not always successfully, to deal with this new domain of human activity.

Neither space nor cyberspace respect national borders. Nations, recognising the changing and more challenging nature of the space environment are nudging towards new understandings and behaviours through Code of Conduct discussions that aim to strengthen space security, initially by increasing levels of trust and confidence. The regulation of cyberspace, in contrast, is very much the preserve of domestic law enforcement agencies. Some are working exceptionally hard to build formal and informal international networks in order to share information which is essential for effective policing. In both environments, situational awareness is lacking and needs to become more comprehensive and timely if confidence and order is to be sustained and strengthened.

There is no evidence that weapons have been placed in space although several nations have anti-satellite (ASAT) missiles that are capable of shooting down satellites in LEO. In doing so, as the Chinese found out to their detriment in 2007, (Johnson-Freese, 2010, pp 9-10) they will almost certainly create more debris which may well be detrimental to the operators of many other satellites in LEO. There is evidence that a number of States have already conducted offensive operations in cyberspace. However, material published in open sources to date has not revealed, **beyond reasonable doubt**, which actor (state, non-state or individual) was responsible.

There certainly have been no admissions of guilt. If a lesser, **balance of probability** test is applied a not unreasonable conclusion is that at the very least China, Israel, Russia and the United States have all conducted offensive operations in cyberspace. Almost certainly there will have been others as well.

The activities of state actors in both space and cyberspace are heavily influenced by intelligence agencies and their culture of secrecy. For how long this situation will remain tenable is open to question in particular in cyberspace. Most critical national infrastructure is owned privately as are most banks. These companies all have a vested interest, in terms of their own business continuity and reputations, to ensure that their networks within cyberspace are secure and resilient. They are also reluctant to publicise successful attacks for fear of scaring off their customers. Intelligence organisations will need to become more open and consultative, especially with the corporate sector, if they are to put what they know to best effect in the interests of their nation. Commander Edward Layton was the senior intelligence officer on the staff of Admiral Nimitz in Hawaii during World War II. He made this point very well:

> Information can be acquired and evaluated until hell freezes over, but it does not become proper intelligence until delivered to the commanders who can make proper use of it. (Layton p55)

Until the 1970s, the principal challenge faced by intelligence agencies was their overall lack of information. Such as they had, often from exceptionally sensitive sources, demanded the most careful protection. With the advent of information from satellites and then the internet, the most pressing question now is how to deal with a data deluge; a deluge that is increasing at an exponential rate. Machines must be invented to sift, catalogue and make initial sense of the mountains of information that are now available. They can 'sense-make' in a way that humans cannot.

Space and cyberspace are profoundly 'dual use' domains and the classification and regulation of these technologies and their associated know-how in order that they do not proliferate to potential adversaries is a continuing challenge for many Western governments. The United States seeks to regulate the export of military technologies and know-how through the International Traffic in Arms Regulations (ITAR). Heavy penalties, sometimes running to hundreds of millions of dollars, have been applied to companies which have been convicted of ITAR violations. Some years ago, the US Congress placed all US developed space hardware, firmware, software and know-how, including for commercial satellites, on the list of controlled goods. This forced a number of countries that previously had purchased particular components for satellites from the US to develop their own, ITAR-free components. Some European satellite manufacturers now advertise some of their products, with pride, as being ITAR free. Meanwhile the US commercial satellite industry languishes because the ITAR restrictions have had the effect of severely limiting a once lucrative export market, especially for telecommunications satellites.

Some further information about future 'dual use' research in Australia is below in the Coda.

CONCLUSION

Space and cyberspace are domains of human activity that share some remarkably similar characteristics in terms of their vulnerability as environments and the fragility of the human activities they support. They are profoundly, and increasingly 'dual use' which is likely to present regulatory difficulties and the possibility does exist the this system could collapse under its own weight.

The space and cyber domains are opaque because adequate situational awareness tools have yet to be developed which nations are prepared to share and trust. Without these tools, the necessary understandings that will be needed, in particular between nations, to ensure that both domains remain safe and secure for all users will be difficult, if not impossible, to broker.

Until the question of attribution in cyberspace is resolved, that domain will remain a risky and potentially dangerous place. Space users are concerned about debris and spectrum access and are aware of the increasing operational risks to satellites especially those in LEO.

Nations and peoples cooperate when they perceive manifest mutual advantage and they are confident that all parties will behave in accordance with some basic norms of decency, transparency and accountability. There is much to be done in both the space and cyberspace domains to ensure that both remain open and accessible to all in pursuit of peaceful and lawful activities.

Coda: Regulating Dual Use Technologies: Recent developments and Implications for Australian Research

Most nations on Earth have a public commitment to disarmament and to reducing and eventually banning weapons of mass destruction (WMD), be they chemical, biological or nuclear in nature. Nations also try to limit the proliferation of delivery mechanisms of such weapons, including missiles. Once these decisions have been

made questions arise about to whom and under what circumstances such technology and know-how might be shared with others. The regime devised by the United States to prevent the unwanted proliferation of military technologies and know-how is known as the International Traffic in Arms Regulations (ITAR). The State Department is responsible for applying the ITAR and the process has become cumbersome and, in some critical areas, self-defeating.

In 1848, Lord Palmerston, famously told the House of Commons:

> Therefore I say that it is a narrow policy to suppose that this country or that is to be marked out as the eternal ally or the perpetual enemy of England. We have no eternal allies, and we have no perpetual enemies. Our interests are eternal and perpetual, and those interests it is our duty to follow.[xiii]

This is commonly paraphrased today as: "Nations have no permanent friends and no permanent enemies. Only permanent interests."

Recently the Australian Parliament passed the *Defence Trade Controls Bill* which is the Australian equivalent of the ITAR.[xiv] In the past decade, the United States has worked to ease the restrictions of the ITAR with respect to its closest allies, the United Kingdom and Australia. In the past, drawing on the logic of Palmerston's dictum, the State Department has treated all foreign entities equally with no special dispensations being given to close allies. This has been burdensome and frustrating from the perspective of the Australian Government and also for Australian defence contractors. There are numerous examples of Australian defence projects being held up due to delays in obtaining ITAR clearance from the United States. The outcome, in Australia's case, is a treaty level instrument that simplifies the release of selected ITAR controlled technologies and know-how from the United States to Australia.

The United States insisted that before the treaty could be signed, Australia would need to establish a robust export control regime of its own to ensure that leakage from the United States via Australia to third parties of ITAR controlled technologies and know-how was minimised and that appropriate punitive measures for those who would break the law were also determined.

The Defence Trade Controls Bill applies directly to research and there is no question that some of the research conducted by ECU's Security Research Institute will fall within the ambit of the Act when it becomes law. There is provision in the Act for a two year trial period during which there will be no prosecutions and efforts will be made to devise straight-forward processes that will quickly alert researchers to the need to obtain approval to release research results into the public domain. [xv] The Act will place an additional, possibly quite heavy burden on universities and other research organisations, including some research conducted by private companies.

REFERENCES

Allison, G.T. *Essence of Decision: Explaining the Cuban Missile Crisis*, Little Brown, Boston, 1971.

Biddington, B & Sach R.H. *Australia's Place in Space: Towards a National Space Policy*, Kokoda Foundation, Canberra, 2010

Hansard's Parliamentary Debates. 3rd series, vol. 97, House of Commons, United Kingdom

Jasper, S. (ed) *Conflict and Cooperation in the Global Commons: A Comprehensive Approach to International Security*, Georgetown University Press, US, 2012.

Johnson-Freese, J. *Heavenly ambitions: America's Quest to Dominate Space*, University of Pennsylvania Press, US, 2009.

Layton, E.T. *"And I Was There: Pearl Harbor and Midway – Breaking the Secrets*, Morrow, New York, 1985

Rumsfeld, D. (Chair) *Commission to Assess United States National Security Space Management and Organization*, Report submitted to Congress in January 2001

Web sources

www.airforcetimes.com

www.consilium.europa.eu

www.defense.gov

www.fas.org

www.google.com.au

www.nytimes.com

www.oosa.unvienna.org

www.reachingcriticalwill.org

www.spacex.com

www.virgingalactic.com

---

[i] http://www.spacex.com

[ii] http://www.oosa.unvienna.org/oosa/en/SpaceLaw/outerspt.html, accessed 4 Nov 2012.

[iii] See http://www.oosa.unvienna.org/

[iv] Lynn, W.J., Deputy Secretary, US Department of Defense, in remarks to a U.S. Strategic Command space symposium in Omaha, Nebraska, quoted in *Space Requires New Thinking, Practices, Lynn Says, by* Terri Moon Cronk, American Forces Press Service, 3 November 2010. See: http://www.defense.gov/news/newsarticle.aspx?id=61544, accessed 4 Nov 2012.

[v] http://www.nytimes.com/2009/02/12/science/space/12satellite.html?_r=0

[vi]http://www.google.com.au/imgres?imgurl=http://www.gearthblog.com/images/images209/debris.jpg&imgrefurl=http://www.gearthblog.com/blog/archives/2009/02/satellite_collision_debris_tracking.html&h=498&w=600&sz=73&tbnid=KuzYfgYkA7r2DM:&tbnh=90&tbnw=108&prev=/search%3Fq%3Dsatellite%2Bcollision%2B2009%26tbm%3Disch%26tbo%3Du&zoom=1&q=satellite+collision+2009&usg=__KvpTalkCuWFvkMzm-9Saxk-FVrQ=&docid=MPhqBs_ADfWZyM&sa=X&ei=w9WWUN6_B6qziQeVxICwDQ&ved=0CEUQ9QEwBg&dur=1214

[vii] http://www.virgingalactic.com/

[viii] http://www.fas.org/nuke/control/paros/index.html and http://www.reachingcriticalwill.org/resources/fact-sheets/critical-issues/5448-outer-space

[ix] http://www.consilium.europa.eu/uedocs/cms_Data/docs/pressdata/EN/foraff/130649.pdf

[x] Roston, A. U.S.: Laws of war apply to cyber attacks, *Air Force Times, September 18, 2012* http://www.airforcetimes.com/news/2012/09/dn-laws-of-war-apply-cyber-attacks-091812/

[xi] Garamone, J. Panetta Spells Out DOD Roles in Cyberdefense *American Forces Press Service, October 11, 2012* http://www.defense.gov/news/newsarticle.aspx?id=11818/

[xii]http://www.google.com.au/publicdata/explore?ds=d5bncppjof8f9_&met_y=it_net_user_p2&tdim=true&dl=en&hl=en&q=world+internet+users

[xiii] Speech to the House of Commons (1 March 1848), *Hansard's Parliamentary Debates. 3rd series*, vol. 97, col. 122.

[xiv] http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r4700

[xv] http://www.theaustralian.com.au/higher-education/defence-bill-amendment-dumped/story-e6frgcjx-1226507419757