ESPI
European Space Policy Institute

ESPI PERSPECTIVES 56

Is There Space for the UN? Trends in Outer Space and Cyberspace Regime Evolution

Larry MARTINEZ, Department of Political Science, California State University

Until the 1980s, outer space and cyberspace (i.e. telecommunication) were accessible predominately to governmental entities or their licensed monopolist operators, an arrangement that enjoyed tight congruencies with long-standing UN jurisdictional competencies and governance mechanisms. By the late 1980s, technological and neo-liberal regulatory trends, shifts in strategic doctrine and growing concerns about orbital and spectrum sustainability emerged as salient factors requiring a re-thinking of how to manage and regulate the outer space and cyberspace realms being used and populated by an increasingly diverse range of military, civilian and commercial entities and services. In contrast to environmental regimes (e.g. law of the sea, Arctic, climate change and biodiversity, among others) that have steadily expanded the range of their legal and institutional jurisdictions within the UN system, the same cannot be said for the actions of the scientific-technological powers, which show a mounting willingness to develop mechanisms for outer space and cyberspace governance outside of the UN system. This paper argues that the seamless technological integration of space systems with cyberspace infrastructures to achieve goals expressed in cyberwar strategic doctrine is also acting to merge the outer space-cyberspace governance domains through a process of ad hoc agreements outside conventional UN legal mechanisms. The on-going negotiations both within and between governments over the European Union's Code of Conduct for Outer Space Activities is but the latest example of this trend.

1. A Fundamental Shift in the Locus of Governance

Formerly governed as separate and distinct realms by treaty frameworks established within the UN system, outer space and cyberspace are emerging into the 21st Century as an increasingly inter-meshed governance regime outside the UN system and its conventional legal mechanisms. This transformation was the subject of a speech delivered on 10 September 2010 by General James E. Cartwright, Vice-Chairman of the U.S. Joint Chiefs of Staff. In his remarks, General Cartwright emphasised how the newly established Cyber Command (USCYBERCOM) underlined a growing recognition by the U.S. Department of Defence that outer space and cyberspace "together" constitute a unique technologically created domain that will be a prominent locus for international strategic, political and economic power competition during the 21st Century.[1] General Cartwright emphasised that strategic doctrine and war fighting were rapidly evolving into a "combined space-cyberspace domain"[2] propelled by technological and commercial trends towards seamless integration of internet capabilities into space satellite systems. These globe-encompassing infrastructures in space for military and civilian navigation, reconnaissance, data communications, broadcasting, financial and banking functions, among a myriad of other services with dual military and civilian applications, represent both a prime means to project power, as well as dependencies and vulnerabilities. Cartwright's speech pointed out that the growing military presence in outer space is occurring simultaneously within a "cyberwar"

1 Author's notes taken at: University of Nebraska. 3rd Annual Space and Cyber Conference, 9-10 Sept. 2010, Washington DC.

2 Butler, A. "Better Late Than Never.". Aviation Week and Space Technology 11 Apr. 2011: 48.

strategic shift, taking place within the military establishments of not only the United States, but of many other military powers as well, that calls into question many long-standing jurisdictional and institutional boundaries defined by the UN and traditionally employed to the governance of the global commons.[3]

With responsibilities for both outer space and cyberspace, we see that the UN's International Telecommunication Union (ITU) finds its role stymied by increasing politicisation for significant aspects of communication satellite governance. Since late 2010, a dispute involving Iran's disregard for ITU regulatory procedures for managing geostationary orbital slots used by multi-national communications (and increasingly internet-based) satellites, exposed a number of political vulnerabilities that are eroding the legal credibility of the UN Organisation's regulatory functions.[4] Meanwhile, suspected Libyan jamming of Al Jazeera transponders on an ARABSAT satellite further exposes the ITU's lack of effective enforcement mechanisms.[5]

Addressing the quasi-governmental Internet Corporation for Assigned Names and Numbers (ICANN) on 11 March 2011 in San Francisco, former U.S. President Bill Clinton re-iterated his support for the regulatory direction his Administration took, in creating through a U.S. Department of Commerce Memorandum of Understanding (MoU) a "multi-stakeholder" governance structure for the nascent internet in 1998.[6] ICANN, as a private corporation licensed under the laws of the U.S. State of California, exercises a regulatory authority of global reach, without an international treaty law specifying its jurisdiction. The trend for outer space and cyberspace governance is away from the UN system, a surprising development given the widespread support and even acclaim for the approaches taken to expand conventional demarcations for other "commons" UN regimes, such as the UN Conference for Law of the Sea (UNCLOS), or the International Civil Aviation Organisation's (ICAO) regulatory role for air commerce, or the Nobel Peace Prize awarded to the UN's Intergovernmental Panel for Climate Change.[7]

2. Towards a Cyberwar Governance Regime

An extensive body of research identifies three sets of distinct but inter-meshed factors for evolving the outer space and cyberspace realms away from the conventional UN-oriented regime and towards a more ad hoc governance arrangement dominated by the major technological-scientific powers: (1) technological and regulatory trends, (2) shifts in strategic doctrine, and (3) sustainability issues associated with the utilisation of the outer space and cyberspace. Amplifying the Cartwright thesis, this paper outlines how these three factor sets are inter-meshing into a "cyberwar" governance regime.

Cyberwar blurs legal distinctions defining the outer space and cyberspace legal regimes and calls into question the UN's role in their future evolution.

"Cyberspace" is in this context an inclusive term, encompassing both telecommunication and data networks and services on national and global levels of interconnection, including the myriad of interfaces into public and private infrastructures. "Cyberwar" is more difficult to define. A broad brush definition takes into its purview those electromagnetic activities intentionally directed at disrupting or destructing communication and data infrastructures, including satellites in outer space interconnected to these information infrastructures. Even with a more narrow definition, specifically focused on data networks and attached control mechanisms, the operationalisation of cyberwar is blurring legal distinctions defining the outer space and cyberspace legal regimes and it is concomitantly also calling into question the UN's role in the future evolution of the outer space and cyberspace regime(s). This is exemplified in a *Los Angeles Times* editorial from January 2011, pointing out:

> *… so Stuxnet doesn't provide a blueprint for wreaking havoc on US nuclear plants or financial institutions. Nevertheless, it's hard to ignore the signs that a new kind of arms race has started, one that goes beyond the denial-of-service attacks and corporate espionage that hackers allegedly conducted, either at the direction*

3 Author's notes from: University of Nebraska Space and Telecommunications Law Programme. 3rd Conference on Space and Cyber Law, 9-10 Sept. 2010, Washington DC.

4 De Selding, Peter B. "Iran's Claims About Satellite Service Try International Regulatory Regime". Space News 11 Apr. 2011: 1.

5 Briel, R. "Al Jazeera Blames Libya for Jamming". Broadband TV News 21 Feb. 2011 http://www.broadbandtvnews.com/2011/02/21/al-jazeera-blames-lybia-for-jamming/.

6 Author's notes: ICANN Plenary Meeting. San Francisco. 16 March 2011.

7 The 2007 Nobel Peace Price was awarded to former US Vice-President Albert Gore Jr., and the UN Intergovernmental Panel for Climate Change. http://nobelprize.org/nobel_prizes/peace/laureates/2007/press.html.

> *of or in support of their governments, against Estonia in 2007, the former Soviet republic of Georgia in 2008 and Google in 2009.*
>
> *The thought of such an arms race is troubling for at least two reasons. The first is that we don't know how the existing international laws and treaties that govern conventional conflicts would apply to cyberwar, if at all. For example, what constitutes an attack, how can anyone tell who's responsible, and what kind of response is justified?* [emphasis added][8]

Let's now briefly examine the three sets of factors that may explain the trend towards an inter-meshed cyberwar governance regime, increasingly distinct from conventional UN frameworks. These factor sets will be analysed in greater depth in their subsequent chapters.

3. First Factor Set: Technological and Regulatory Trends

Cyberspace and outer space are technological domains. Created by often spontaneous and serendipitous technological discovery and innovation, they expand as new realms of human activity open up, often far in advance of governance mechanisms and institutions. At the same time, they are arenas for international competition, effecting often far-reaching shifts in the configuration of world power. Furthermore, as Professor Debora Spar in her book, *"Ruling the Waves: From the Compass to the Internet, A History of Business and Politics along the Technological Frontier"* points out, technological innovation and regulatory governance evolve through distinct phases defined by a pivot point, where the dominant industrial actors realize that market anarchy (open resource "commons" such as the radio spectrum and the "open" internet) works against their long-term commercial interests.

Cyber-conflict (including the intentional hacking and disruption of corporate IT infrastructures) inserts technological anarchy into even highly regulated markets, thereby reducing corporate sector willingness to rely on governmental regulatory mechanisms and institutions as Spar's model would predict.[9] Spar's observations about resource commons dispute set the stage for the discussion of the second and third factor sets described below.

4. Second Factor Set: Shifts in Strategic Doctrine

From the very beginning of the modern space age with the launch of Sputnik in 1957, outer space has been the "high ground" for superpower strategic doctrine and power projection. What is changing is the near seamless integration of military space systems into cyberspace infrastructures for both military and civilian applications and commercial services, as exemplified by satellite-based navigation.

The question remains whether deterrence can be a viable doctrine in an operational battleground where attributing attacks is extremely ambiguous.

Cyberwar strategic doctrine is quickly evolving. On 16 May 2011, the United States Government released its *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*.[10] A few weeks later, on 15 July 2011, the U.S. Department of Defence released its statement of strategic policy[11] designed to update long-standing nuclear weapons' deterrence doctrine developed during earlier Cold War eras, to the current era in which cyberattacks witness particular prominence.[12] In an article published by Aviation Week and Space Technology on 23 April 2011, the ambiguities of cyberwar as applied to nuclear-era deterrence and strategic doctrines become readily apparent:

> *The rules of war when applied to cyberconflict also are still poorly defined. Does an attack on a NATO member trigger the alliance's Article 5 collective defense mandate? What are the rules of engagement when it comes to counterstrike? Is an adversary's banking system or power grid a legitimate target?*[13]

In the cyberwar realm, the evolution of strategic doctrine will increasingly focus on a wide range

8 "Will the Cyber Worm Turn?" Los Angeles Times 23 Jan. 2011: A29.

9 Spar, D. *Ruling the Waves: From the Compass to the Internet, A History of Business and Politics along the Technological Frontier*. New York: Harcourt Inc., 2011: 10.

10 The White House. "International Strategy For Cyberspace: Prosperity, Security, and Openness in a Networked World". Washington DC May 2011. http://www.whitehouse.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf.

11 US Department of Defence. "Department of Defence Strategy for Operating in Cyberspace". Washington DC 15 July 2011. http://www.defense.gov/news/d20110714cyber.pdf

12 Sanger,D.E. and Bumiller E. "Pentagon Will Consider Cyberattacks Acts of War." New York Times 1 June 2011: A10.

13 Fulghum, D. A. and Wall, R. "Cybersleuthing: Threats Will Change as New Forensic Techniques Provide Attribution". Aviation Week and Space Technology 23 Apr. 2011: 44.

of disruptive to destructive cyberattacks involving space systems, from the intentional jamming of satellite networks for broadcast services to sustained cyber-assaults against an adversary's financial system, electrical power grid, or military command infrastructures.[14]

5. Third Factor Set: Challenges to Outer Space and Cyberspace Sustainability

Outer space and cyberspace are facing growing challenges to their long-term sustainability, a threat perceived particularly acutely by the military establishments of major space powers, merging jurisdictional approaches to a combined cyber war domain. "Sustainability" in this context pertains to the costs of access to and use of outer space and cyberspace domains (risk being a major component of cost). The sustainability threat takes two main forms: physical (space debris) and electromagnetic (spectrum interference, targeted electromagnetic jamming, malware weaponisation and directed energy weapons).

Space Debris

In outer space, the mathematical laws of orbital physics and atmospheric drag dictate the length of time an object, whether an operating satellite or a wayward bolt or paint flake, will remain in orbit around the Earth.[15]

Ground-based radars, capable of seeing objects larger than one centimetre, can track less than 20,000 of the estimated 600,000 manmade pieces of space junk, while that number is steadily growing.

In 2007, the Chinese government destroyed a retired weather satellite by launching an anti-satellite weapon that successfully intercepted it. The collision created thousands of pieces of debris that will greatly endanger other satellites in certain orbital altitudes for hundreds of years. The following year, U.S. government conducted its own anti-satellite test in a much lower orbit, with fewer long-term potential consequences due to the collision's lower altitude.[16]

However widespread, the reaction to the Chinese anti-satellite test paled compared to the world's space community reaction after the shocked realisation that the debris threat literally exploded in 2009, as a functioning Iridium communications satellite was instantly destroyed following a collision with a piece of a Russian booster rocket.[17] The multiplying effect of debris creating more debris invokes the "Kessler Syndrome", according to which entire regions of Earth orbital altitudes will be made unusable by debris concentrations.

Electromagnetic

As every Internet user quickly realises, over one-half of all e-mail is unwanted "spam". More seriously threatening is the growing number of cyber attacks on information networks that conduct global and national financial transactions, governmental operations, and the myriad of economic, political and societal functions now entrusted to literally billions of computers and mobile devices. Analogous to the problem of space debris, the online world is dealing with congestion and disruption, as cyberspace becomes an increasingly important element of national infrastructures and power projection in the international arena. "Cyber war" now joins spam, viruses, Trojan horses and worms, as deliberate attempts to disrupt communications on the internet and other data, financial, and infrastructure-critical computer networks.

The potentiality of cyber war became a strategic reality in 2010, as "Stuxnet" infiltrated the Iranian nuclear facilities and disrupted and/or disabled hundreds of high-speed centrifuges.[18] The evident, but largely unconfirmed, success of the *Stuxnet* virus to disrupt highly secure national security infrastructure points to the growing wave of national defence establishments attempting to weaponise cyberspace.[19] The future will provide more focused and effective uses of cyberspace weaponry that will disrupt vital infrastructures, financial systems and security establishments, while making access to the internet unreliable and the information there increasingly antagonistic to transparency and

---

14 Author's notes from the USSTRATCOM Cyber and Space Symposium: *Space and Cyber: New Challenges, New Opportunities*, November 15-17, 2011, Omaha, Nebraska.

15 Welly, N. "Enlightened State-Interest -A Legal Framework for Protecting the 'Common Interest of All Mankind' From Hardinian Tragedy". Journal of Space Law 36.1 (Summer 2010): 273. http://www.spacelaw.olemiss.edu/jsl/pdfs/articles/jsl-36-welly.pdf.

16 Covault, Graig. "China's Antisatellite Weapon's Test to Intensify Milspace Debate". Aviation Week and Space Technology 21 Jan. 2007: 24.
Shanker, Thom. "Missile Strikes a Spy Satellite Falling From Its Orbit". The New York Times 21 Feb. 2008: A15.

17 Marks, Paul. "Satellite Collision 'More Powerful Than China's ASAT Test'". New Scientist 13 Feb. 2009. http://www.newscientist.com/article/dn16604-satellite-collision-more-powerful-than-chinas-asat-test.html.

18 Fildes, Jonathan. "Stuxnet Worm 'Targeted High-value Iranian Assets'". BBC News 23 Sept. 2010. http://www.bbc.co.uk/news/technology-11388018.

19 Author's notes: Cyber war and Cyberspace Conference. General James E. Cartwright Remarks. 10 Sept. 2010, Washington, DC.

democratic accountability.[20]

Although highly classified, it is possible to discern the outlines of the growing cyber war capabilities that are forming the battlefields of the 21st Century. In the wake of the revelations and disputed origins of the *Stuxnet* virus, *Aviation Week and Space Technology* published the following description of U.S. cyber strategy that appears to go far beyond the "direct connection" mode for cyber attack target access:

> *…The U.S. has been studying and testing associated capabilities. In the "Aurora Test" conducted by Idaho National Laboratory in early 2007, a 21-line package of software code sent from 100 mi. away caused a $1-million commercial electrical generator to generate self-destructive vibrations by rapidly recycling its circuit breakers.* [emphasis added][21]

In other words, conventional means for shielding and protecting vital national assets from cyber war attacks may no longer be as impenetrable as once believed, if the above quote accurately depicts a wireless cyber access capability.

6. Trend Spotting

Does the aforementioned discussion support the argument for an emerging *ad hoc* outer space-cyberspace cyber war regime? The question of who shall set the rules then also arises: would it be the international community as represented by the UN, or the actual users, e.g. corporations or individual governments operating in these technological realms?

Apart from some exceptions, the trend is against a larger UN role in outer space and cyberspace governance.

In general, the UN's role in keeping pace with the expanding realms of outer space and cyberspace entities and services has not been as significant as one might expect. There are several factors working here. First, as outer space and cyberspace technologies proliferated within an environment of liberalised market regulation, commercial firms now seem to prevail on significant aspects of both realms, replacing government authorities or government-licensed monopolists' long-standing domination. In a highly competitive marketplace, any mode of international governance now touches upon proprietary data that firms are very reluctant to share through multilateral governmental fora beyond their control.

Furthermore, by their very definition the technological realms of science and mathematics admit very little diplomatic "wiggle room" that is necessary for large-group compromise. There is the physical reality of collisions in orbit; the internet works or it doesn't.[22]

Two examples from the space debris and internet management arenas illustrate the future trend, away from direct UN role and towards an eclectic private-public "civil society" approach.

Space Debris

Key to the long-term sustainability of the <1,000 Km orbital region is an up-to-date database of space objects which would allow operators to move their endangered satellites out of the path of space debris. With the encouragement of a few key individuals, such as Richard DalBello of Intelsat, the Space Data Association (SDA) was formed in 2009.

This self-financing association of satellite operators from multiple nations also works closely with governmental space authorities to develop guidelines regarding other sustainability measures, such as de-orbiting satellites, or placing them in graveyard parking orbits above the geostationary altitude, so that dead satellites cannot collide or interfere with the operating ones.

Internet Management

The World Summit on the Information Society (WSIS) was authorised by the UN General Assembly Resolution 56/183 (of 21 December 2001) for a two-stage process, held first in Geneva in 2003 and then followed-up by an implementation stage held in Tunis in 2005.[23] Much of the momentum for the WSIS was gathered from the growing unease among many states that their national infrastructures were increasingly dependent on the Internet, the governance of which they did not control.

The U.S. Department of Commerce, seeking to

---

20 Morozov, E. The Net Delusion: The Dark Side of Internet Freedom. New York: Public Affairs, 2011.

21 Fulghum, D. "No Fingerprints: Culprits in the Cyberattack on Iran Are Still Unknown". Aviation Week and Space Technology 4 Oct. 2010: 29.

22 Martinez, L. "Science in Service of Power: Space Exploration Initiatives as Catalysts of Regime Evolution". Air and Space Law, Nov. 2007: 431.

23 World Summit on the Information Society Website: http://www.itu.int/wsis/index.html.

establish a long-term governance structure for the World Wide Web addressing database, licensed in 1998 a private corporation under the State of California laws to manage the registration of internet domain names. The Internet Corporation for Assigned Names and Numbers (ICANN) took on the task of managing the country codes and domain names for Web addressing, a function posing many sovereignty issues that a growing number of countries wanted to see addressed in a UN forum. The Internet Governance Forum (IGF) has attempted to open up the process of internet governance to a more governmental organisational structure, arguing that the current modes for Internet management are less able to directly address governmental concerns.[24] The recently released U.S. Government international policy for cyberspace stresses its goal of maintaining the "multi-stakeholder" orientation for cyberspace governance.[25]

7. Concluding Observations

As in the space debris example, technological imperatives for effective network management resisted WSIS proposals to shift ICANN (and thereby internet) governance to a structure much closer to the conventional UN-ITU organisational process. ICANN is increasingly involved in internet security, as the volume of cyber war attacks mount against internet root servers that manage all internet data traffic. During discussions on internet governance at the ICANN meetings in June 2010 in Brussels and March 2011 in San Francisco, it was very apparent that the organisation's "multi-stakeholder" structure continued to prove itself based on its performance, rather than its legitimation through UN open access.[26] Military concerns and proprietary technologies can create barriers to the openness required by UN based regimes, and in this regard the 1987 Missile Technology Control Regime (MTCR) stands as a leading example.[27] The contention of this paper is that a similar line of factors are influencing the evolution towards a global governance process for outer space and cyberspace that will be increasingly dominated by actors motivated by cyber war concerns and strategies. The highly asymmetrical distribution of national capabilities and vulnerabilities in the cyber war domain will contribute to reducing the incentives to utilise existing UN governance institutions and mechanisms premised on legal precepts of sovereign equality. Instead, we are already observing a move on the part of technologically advanced powers to address their disputes in *ad hoc* governance fora, as the case of the EU Code of Conduct for Outer Space Activities exemplifies.

8. Policy Considerations

The ICANN and Space Data Association are both examples of *ad hoc* governance through multi-stakeholder organisational mechanisms. While a multistakeholder organisational structure matches more closely technological and capability symmetries between the affected entities, its legal basis under international outer space and cyberspace law remains unsettled. As cyberwar continues to embed itself ever deeper in outer space and cyberspace establishments, a "best practices" research effort should be launched to foster wider awareness of both the promise and the challenge that the multi-stakeholder governance regime poses against effective outer space and cyberspace governance, in the era of cyberwar.

[24] Internet Governance Forum Website: http://www.intgovforum.org/cms/.

[25] The White House. "International Strategy For Cyberspace…": 10.

[26] "Legitimation through performance" in the context of global governance was discussed by Professor Karl Kaiser in his article, "Globalisierung als Problem der Demokratie". Internationale Politik April 1998.

[27] Missile Technology Control Regime Website: http://www.mtcr.info/english/index.html.

ESPI
European Space Policy Institute

Mission Statement of ESPI

The European Space Policy Institute (ESPI) provides decision-makers with an informed view on mid- to long-term issues relevant to Europe's space activities. In this context, ESPI acts as an independent platform for developing positions and strategies.

Available for download from the ESPI website
www.espi.or.at

Short title: ESPI Perspectives 56
Published in January 2012

Editor and publisher:
European Space Policy Institute, ESPI
Schwarzenbergplatz 6 • A-1030 Vienna • Austria
http://www.espi.or.at
Tel: +43 1 7181118-0 / Fax: -99
Email: office@espi.or.at

ESPI Perspectives are short and concise thought or position papers prepared by ESPI staff as well as external researchers.

Any opinion expressed in this ESPI Perspective belongs to its author and not to ESPI.
The author takes full responsibility for the information presented herein.