The Legal Dimensions of Cyber-Conflict with Regard to Large Satellite Infrastructures and Constellations

Larry F. Martinez[*]

Abstract

Proposed large *digital* satellite infrastructures and constellations in low-earth orbits are designed to be highly integrated into Internet networks, thereby posing significant challenges to established legal and regulatory precedents for mitigating cyber-interference and cyber-conflict issues. Based on the 1960s Outer Space Treaty and subsequent 1970s space treaties, the initial legal framework addressed regulatory issues for *analog* satellite systems consisting primarily of individual governmental and civilian satellites in geostationary, polar, or sun-synchronous orbits, buffered from terrestrial telecommunications disruptions by highly secure earth stations. Starting in the 1990s, launches of large constellations of navigation and low-earth orbit communications satellites presaged a shift to new forms of *digital* satellite-based space communication networks directly integrated into terrestrial Internet networks servicing billions of smartphones and computers. Inherent Internet vulnerabilities makes satellite-based Internet networks and all who rely on them increasingly vulnerable to direct disruption by private hackers and/or massive state-sponsored cyber-warfare assaults. This paper examines how the international legal regime for outer space may evolve in response to cyber-conflict, with a strong likelihood that the outer space regime will increasingly mirror the "soft law" regime currently characterizing Internet regulation in large part owing to cyber-vulnerabilities and proprietary technologies.

1. Introduction: The Internet Is Disrupting Outer Space Governance

2017 will mark the 60th anniversary of the orbiting of the first artificial earth satellite, *Sputnik,* and the beginning of the modern era of space exploration. Although space exploration and exploitation cannot function without reliable and interference-free telecommunications links, the initial outer space legal

* Department of Political Science, California State University, 1250 Bellflower Blvd., Long Beach, CA, 90840-4605, USA, larry.martinez@csulb.edu.

regime was founded upon "hard" (i.e., legally binding) law treaties drafted by the UN Committee on Peaceful Uses of Outer Space (UNCOPUOS) in the 1960s-1970s that, for the most part, did not specifically address legal aspects of space *telecommunications* regulation.[1] Space telecommunications, including radio spectrum allocations and management, was specifically tasked to the International Telecommunication Union (ITU) through its constitutive charter and radio regulations as legally binding agreements beginning in 1963.[2]

The ascendancy of telecommunications-related services as the prime application of outer space technologies prompted the UNCOPUOS to draft and the United Nations General Assembly in the 1980s to adopt *non-binding* resolutions addressing concerns of countries regarding remote sensing and direct TV broadcasting from space satellites, concerns that were not specifically addressed in the hard law space treaties.[3] The ITU's periodic World Radio Conferences promulgated the Radio Regulations, "hard" law rules that allocated and managed frequency bands for interference-free satellite operation, while UNCOPUOS-drafted treaties established legal "rules of the road" for accessing and using the orbital regions for the "benefit of all mankind." Most significantly, however, the legal contours of the UNCOPUOS-ITU regime closely fit the technological configurations of the first generations of "analog" space telecommunications systems.

---

1 *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. *Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space,* Adopted by the General Assembly in its resolution 2345 (XXII), opened for signature on 22 April 1968, entered into force on 3 December 1968. *Convention on International Liability for Damage Caused by Space Objects* (resolution 2777 (XXVI), annex) – adopted on 29 November 1971, opened for signature on 29 March 1972, entered into force on 1 September 1972; *Convention on Registration of Objects Launched into Outer Space* (resolution 3235 (XXIX), annex) – adopted on 12 November 1974, opened for signature on 14 January 1975, entered into force on 15 September 1976. The 1979 *Moon Agreement* has been ratified by only a small number of states (16) and is not considered to be fully in force (*Agreement Governing the Activities of States on the Moon and Other Celestial Bodies*, Adoption by the General Assembly in its resolution 34/68 on 5 December 1979, opened for signature on 18 December 1979, entered into force on 11 July 1984). Source: http://www.unoosa.org/documents/pdf/spacelaw/treatystatus/AC105_C2_2016_CRP03E.pdf (Accessed on July 20, 2016).

2 International Telecommunication Union, *Final Acts of the Extraordinary Administrative Radio Conference to Allocate Frequency Bands for Space Radiocommunication Purposes*, Geneva 1963. Source: http://www.itu.int/dms_pub/itu-s/oth/02/01/S020100004E4001PDFE.PDF (accessed on July 20, 2016).

3 "Other Agreements," Source: http://www.unoosa.org/documents/pdf/spacelaw/treatystatus/AC105_C2_2016_CRP03E.pdf (accessed on July 20, 2016).

Using analog modulation techniques (i.e., amplitude modulation or frequency modulation, among others) for relaying voice, sound, or video, geostationary (or elongated polar orbiting "Molnya") satellites were configured as "bent pipes" that re-transmitted back to earth what they received. In other words, the communications payload (ITU) of a satellite was distinct in a technological and regulatory sense from the physical engineering platform of the satellite itself as launched and placed into orbit (UNCOPUOS).

It is important to note that satellites from the very beginning of the space age employed analog payloads and digital control technologies. While satellites through the 1990s relied on *analog* techniques for information relay amongst earth-bound analog network providers, the control over satellite functions was accomplished through highly secure telemetry links digitally "piggybacking" on analog pathways between large earth stations and the satellites. Significantly, the analog "payload" – the actual profit-generating communications services whether TV, voice, or other services – was analog and technologically dissimilar from the digital telemetry pathways used for controlling the satellites. The shift to all-digital satellites that began in the late-1980s, accelerated not only satellites' ability to provide in orbit switching and Internet services to widely-dispersed users, but also exposed satellites to the same enormous cyber-vulnerabilities that Internet connectivity poses to all networked users. To understand why the Internet is insecure one must look at its origins.

The Internet began in 1969 as an experimental program conducted by the U.S. Department of Defense to develop a digital networking technique called "packet switching" that could allow dissimilar computers at university and governmental research facilities to seamlessly exchange data. Key to the ARPANet's successful deployment in the 1970s and 1980s was the TCP/IP (transmission control protocol/Internet protocol) software protocol that allowed dissimilar computer networks to seamlessly exchange data through voluntary adoption of the TCP/IP interconnection. Packet-switching de-centralized network administration as links were selected "on the fly" by the network's routers, allowing the network to constantly exploit unused capacity while at the same time correcting for any disturbances or inoperative links. As a network utilized initially be the close community of computer researchers, a high degree of trust supported open and transparent network software such as the TCP/IP inter-connection protocols. From the very beginning, that openness and transparency highly prized by the computer community also discouraged any fundamental efforts to build in features that would enhance security. In the early 1990s, the ARPANet graduated from the universities and became the "inter-network" or "Internet" as commercial network operators also began to voluntarily interconnect their networks using the TCP/IP protocol. The efficiencies of packet-switching and the ability of the TCP/IP protocol to seamlessly interconnect dissimilar computer networks propelled the Internet's rapid worldwide deployment in the 1990s,

albeit with the security vulnerabilities endemic to an open and transparent network architecture instilled by its computer community origins.
To meet the burgeoning worldwide demand for Internet connectivity, network operators in the late-1990s began to look to satellite manufacturers and operators for innovations beyond conventional geostationary (GSO) satellite configurations that could provide affordable Internet connectivity to over half of the human population living in underserved regions. Beginning with Motorola's *Iridium* system, satellite manufacturers and operators began in the 1990s to propose large, non-GSO, satellite constellations that would, through inter-satellite links, replicate in low earth orbit the Internet's packet-switching network architecture.[4]

2. Large Satellite Constellations

Large satellite constellations, consisting in some proposals of hundreds or even thousands of satellites, are designed to bring low-cost Internet access to underserved regions of the globe, and are now, like the Internet itself, disrupting the long-standing legal and regulatory accommodations between the "hard" law cyber-spatial (telecommunications) and outer space regimes, i.e., the ITU-UNCOPUOS bifurcated regime. Moreover, the growing cyber-vulnerability of Internet-based networks in general, and of large constellation satellite infrastructures in particular, operates as one of the key factors shifting space governance to a "soft" law regime, potentially in a very disruptive fashion more reminiscent of the current trends in the "multi-stakeholder" forums for Internet governance, such as the Internet Corporation for Assigned Names and Numbers (ICANN).[5] Proposed deployments of large Internet-based satellite infrastructures and constellations in low-earth orbits pose three systemic challenges to established legal and regulatory dimensions for cyber-interference and cyber-conflict issues: (1) digital Internet network architectures; (2) spectrum allocations and coordinations; and, (3) threats to reliable operation. Taken together, these three clusters of systemic change mark the merging of the digital "soft law" governance model for telecommunications into the pre-existing analog "hard law" regime for outer space. Outer space will be governed increasingly as "cyberspace."

4 See, John Bloom, Eccentric Orbits, Atlantic Monthly. Source: http://www.wsj.com/articles/the-fall-and-rise-of-iridium-1464980784 (accessed August 26, 2016).

5 ICANN was established in 1998 as a private non-profit corporation under California law. See, Wikipedia, "ICANN," Source: https://en.wikipedia.org/wiki/ICANN (accessed on August 24, 2016).

2.1. Digital Internet Network Architectures

Cyberspace and outer space are areas of human activity created by technology. Governance, as a combined effort by authorized entities to promulgate, enforce and interpret principles, rules, and regulations affecting the long-term use of cyberspace and outer space, must, from the outset, take technological factors in account. While technological determinism is usually an over-simplification, the emergence of large constellation satellite infrastructures represents a technological evolution with far-reaching implications for governance.

A major component of the Internet's disruptive influence on the evolution of outer space governance is due to its very nature as a *digital* telecommunications infrastructure. In replacing the pre-existing *analog* infrastructures, the Internet's packet-switched digital network architecture also brought with it a highly decentralized and non-governmental management arrangement that represents the polar opposite from the earlier governance regimes during the state-monopolist analog era of telecommunications (both terrestrial and space) regulation that was in effect during the promulgation and entry into force of the "hard" law space treaties in the 1960s-1970s. One other systemic difference marks the digital era as different from the analog with regard to cyber-conflict. While it was possible to tap into analog networks for purposes of monitoring, there was almost no opportunity for "hacking" the network's electro-mechanical analog components. With the introduction of computerized electronic switches in the late-1960s, some parts of the public-switched network converted to digital technology and thereby became a preferred target for "hackers." In the early 1970s, two college students in California used inexpensive hobbyist electronic components to mimic digital signaling tones in their "dorm room prank" manipulations of AT&T's worldwide "Touch-Tone" digital switching technology. These students later went on to establish the Apple computer company.[6]

Analog telecommunication techniques require an "always-on" discrete communication pathway between communicators. The dial tone heard on conventional landline telephone systems indicated to the subscriber that the copper wire link was operating to the network provider's central office switch. That electro-mechanical switch created discrete pathways between subscribers or between subscribers connected through a series of central office switches. The economics of "natural" monopolies dictated a highly centralized structure for network operation, administration, and regulation. Satellites were "bent-pipe" extensions of the existing terrestrial analog circuits between switches and subscribers. In most cases, the same governmental telecommunications monopolist (usually the Poste, Telegraph

6 See, *Wikipedia*, "Steve Wozniak," Source: https://en.wikipedia.org/wiki/Steve_Wozniak (accessed: July 26, 2016).

and Telephone – "PTT") represented a particular state party in the promulgation of the ITU Radio Regulations or the UN's space treaties regulating use and operation of satellite networks. In an operational sense as well, governmental monopolist operators dominated both the major satellite communication providers (INTELSAT, Intersputnik, INMARSAT, EUTELSAT, ARABSAT, among others). Networked access to GSO satellite links was accomplished through large, very expensive earth stations, owned and operated by the very same governmental-monopolist entities that represented the state parties in the ITU and UN negotiations leading to "hard" law treaties.

Advances in computer technologies and software also brought about dramatic reductions in information transaction costs predicted by "Moore's Law."[7] Translating analog information into digital ones and zeros allowed network operators to exploit computer efficiencies that obsoleted centralized analog switches. Voice, video and data could be electronically packaged into digital "packets" that could be sent between the computerized routers constituting what became the inter-network network, or the "Internet." The nearly seamless integration of computing with network interconnections proceeded through an administrative structure legitimized by the binary performance of the inter-connection (does it work, yes or no?).

The Internet, in contrast to analog networks, is the regulatory product of a U.S. governmental "hands-off" developmental process conducted by universities working with private digital network providers and data processing companies. The horizontal multi-stakeholder[8] *ad hoc* regulatory process that grew up around the Internet is out of synch with a vertical and very hierarchical regime structure among governmental-monopolist analog network operators that sought to maintain their dominance in the institutions constituting the state-centric cyberspace and outer space legal regimes. However the plate tectonics of regulatory evolution are exposing legal faultlines between the Internet and the state-centric regime.

These faultlines were recently brought to light as the UNCOPUOS, the chief global forum for discussing and formulation of the regulatory "rules of the

7 Gordon Moore, co-founder of Intel Corporation predicted that every 18 months the density of electronic components on a chip would double while the costs would halve. By and large, Moore's prediction has held as technological advances continue to make possible ever more capable chips with lower costs per operation. See, Wikipedia, "Moore's Law," https://en.wikipedia.org/wiki/Moore%27s_law (accessed July 25, 2016).

8 The Internet Corporation for Assigned Names and Numbers (ICANN) is perhaps the most visible regulatory entity for the Internet. At its 56th meeting (June 27-30, 2016) in Helsinki, Finland, the United States government officially notified ICANN about its decision to formally relinquish direct governmental oversight for the Internet root server administration. See, https://www.icann.org/en/system/files/files/icann56-technical-report-18jul16-en.pdf (accessed July 20, 2016).

road" for outer space met for its 59th meeting from June 8-17, 2016 in Vienna, approving the first guidelines for long-term sustainable use of outer space.[9] Along with its sister UN organization responsible for frequency management for satellites, the International Telecommunication Union (ITU), both organizations sponsored meetings in June 2016 focusing on efforts being taken by international community in its attempts to grapple with a fundamentally altered regulatory environment for earth's orbital regions with significant implications for larger security issues, including those stemming from cyber-related challenges posed by large constellations of Internet-connected satellites at low earth orbital altitudes.

2.2. Spectrum Allocations and Coordinations

Beginning in the analog era of the 1960s-1980s, most public-switched telecommunications infrastructures utilizing geostationary low-power satellites were connected through massive terrestrial antenna facilities operated by governmental monopolists (epitomized by the INTELSAT "Standard A" earth station[10]). As noted above, satellites were "bent-pipes" allowing the interconnection of discrete analog communication pathways between central office switches dispersed over the satellite's hemispheric footprint. ITU World Radio Conferences allocated spectrum and specified the procedures for coordinating simultaneous use of frequency bands among contending users (chiefly in the C-, Ku-, and Ka-frequency bands) of satellite systems in the geostationary orbit. The ITU Radio Regulations were binding "hard" law legal agreements that assigned specific rights to interference-free spectrum use and geostationary orbital slots. Cases of spectral interference would be "coordinated" among the different governmental monopolist claimants to a particular spectrum band and orbital slot(s) as specified by the ITU Radio Regulations and other ITU constitutive agreements.[11]

As noted above, the transition to digital telecommunications networks brought with it a growing diversity of users as governmental "natural" monopolies were broken up in the 1980s-1990s in a wave of telecommunications reforms undertaken first by the leading technology nations and gradually by industrializing countries intent on capturing the

9 United Nations Committee on Peaceful Uses of Outer Space (UNCOPUOS), *Guidelines for the long-term sustainability of outer space activities: Conference room paper by the Chair of the Working Group on the Long-term Sustainability of Outer Space Activities,* June 16, 2016 (A/AC.105/2016/CRP.17).

10 See, *Intelsat,* "A Practical Introductory Guide on Using Satellite Technology for Communications," Source: http://www.intelsat.com/wp-content/uploads/2013/01/5941-SatellitePrimer-2010.pdf (accessed August 1, 2016).

11 See, International Telecommunication Union, "Collection of the Basic Texts of the International Telecommunication Union adopted by the Plenipotentiary Conference," Source: http://www.itu.int/pub/S-CONF-PLEN-2015 (accessed July 26, 2016).

Internet's dynamism for their own nascent information economies.[12] What used to be an analog networks' "old boys' club" of monopoly providers, had become a digital "free for all" as computer, software, and networking firms competed to bring the Internet's cornucopia of information to customers' personal and workplace computers initially using wired network connections. Moore's Law continued to accurately track the shrinking digital chip with the result that cellphones became hand-held ubiquitous computers by the late-1990s. However, limitations in the bandwidth available for public-switched cell networks severely limited the information handling capabilities of the increasingly powerful handheld devices now flooding the market. Into the 21st Century, the digital smartphone revolutionized the concept of connectivity and spectrum use. Today, peta-bytes (a million gigabytes) of data[13] are exchanged daily between an estimated billion+ connected smartphones worldwide using "Wifi" and cellular spectrum, increasingly seen as encroaching on those ITU allocations long used by geostationary satellite networks.

So-called "Wifi" spectrum exemplifies the shift in electromagnetic governance brought on by the Internet and computer revolutions. The ITU in 1947 allocated spectrum for short distance applications, including use of the 2.4 GHz band for microwave ovens.[14] In 1985, the ISM (Industrial, Scientific and Medical) radio bands, were released for use by unlicensed entities by order of the U.S. Federal Communications Commission (FCC).[15] Using digital radio "spread spectrum" modulation techniques, manufacturers of networking equipment were able to create a multi-billion dollar worldwide market in Wifi devices by the early 21st Century. Spread spectrum is a digital radio technique of placing information into electromagnetic waves that may directly overlay other waves, relying on software to extract and decipher the embedded information by the receiver. As such, spread spectrum represents a radical departure from conventional analog spectrum governance that sought to avoid interference by limiting use of frequencies to one authorized user in a particular geographical location. Today, billions of devices interconnect wirelessly in the ISM radio bands used by Wifi equipment, mainly at 2.4 GHz

12 See, International Telecommunication Union, "World Summit on the Information Society," Source: http://www.itu.int/net/wsis/tunis/ (accessed on July 26, 2016).

13 See, "Internet Live Stats," Source: http://www.internetlivestats.com/ (accessed July 25, 2016).

14 See, *Wikipedia*, "ISM Band," Source: https://en.wikipedia.org/wiki/ISM_band (accessed July 27, 2016).

15 See, *FCC*, "Authorization of Spread Spectrum Systems Under Parts 15 and 90 of the FCC Rules and Regulations". Federal Communications Commission of the USA. June 18, 1985. Archived from the original (txt) on September 28, 2007. Retrieved 2007-08-31. Source: *Wikipedia*, "Wifi," footnote 3. Source: https://en.wikipedia.org/wiki/Wi-Fi (accessed July 27, 2016).

and 5 GHz. The regulatory dominance of the monopolist user was coming to an end.

The June 2016 ITU symposium focusing on the interference issues facing satellite operators outlined the concern whether the ITU's spectral governance can sustainably accommodate both terrestrial and space spectrum needs for the coming decade(s).[16] Occurring during the same week as the UNCOPUOS meeting in Vienna, both organizations grappled with governance issues challenging reliable operation of satellite systems stemming from physical as well as electromagnetic sources of conflict.

2.3. Threats to Reliable Operation

2.3.1. Physical Threat: Space Debris

In the broadest, long-range historical view, large satellite constellations have always been an intriguing option for telecommunications providers seeking to exploit the "high ground" of space for reliable worldwide links. Probably the most extreme example of a "passive" large satellite constellation was the Project West Ford launched in 1961 (assumed failure to deploy) and 1963 that deposited "millions" of 1.8 cm copper wires into a 3,500 kilometer polar orbit.[17] Each copper wire was designed to operate as 8 GHz dipole antennas for the purpose of reflecting radio waves between terrestrial communicators. The successful experiments likewise in the early 1960s with "active" satellite relays in LEO (Telstar) and at geosynchronous altitudes (Syncom) obsoleted further plans to test large satellite constellations until the early 1990s, when Motorola presented its proposal for what became the 66-satellite Iridium LEO network. Iridium was followed by deployments of Globalstar and Orbcomm LEO satellite constellations beginning in the 1990s.[18] Although the three LEO constellations eventually demonstrated their ability to provide a cellular-like service to underserved areas, their customer appeal was limited due to terrestrial cellular's rapid evolution to smaller and Internet-capable handsets.

Teledesic was the first LEO constellation specifically designed for Internet connectivity.[19] Its ambitious aims to provide global Internet access through a

16 See, author's notes, and, International Telecommunication Union, "Interference-Free Satellite Frequency Spectrum: Myth or Reality in 2016," held June 13-14, 2016 at ITU Headquarters, Genève, Switzerland. Source: http://www.itu.int/en/ITU-R/space/workshops/SISS-2016/Pages/default.aspx (accessed July 26, 2016).

17 Hanson, Joe. (2013) "The Forgotten Cold War Plan That Put A Ring Of Copper Around The Earth," *Science*, August 13, 2013. Source: http://www.wired.com/2013/08/project-west-ford/ (accessed July 21, 2016).

18 Wikipedia, "Globalstar," Source: https://en.wikipedia.org/wiki/Globalstar (accessed: July 21, 2016); "Orbcomm," Source: https://en.wikipedia.org/wiki/Orbcomm_(satellite) (accessed July 21, 2016).

19 Wikipedia, "Teledesic," Source: https://en.wikipedia.org/wiki/Teledesic (accessed on July 21, 2016).

constellation of up to 840 LEO satellites was suspended in 2002, but not before receiving a worldwide spectrum allocation in the Ka-band from the ITU.[20]

Although not a cyber problem *per se*, hundreds or even thousands of small satellites pose a physical challenge to the legal goal set by the Outer Space Treaty for long term sustainable access for all countries. The problem is trash, orbital trash called space debris that now threatens to make unusable huge swaths of the most favorable near-earth orbital regions between 300 and 2000 kilometers altitude. Thousands of pieces of debris were created by a Chinese anti-satellite (ASAT) test in 2007 that blew up a retired Chinese satellite and the benign neglect that marked international discussions about space debris up to that point. Following the 2009 collision between a Russian rocket fragment and a perfectly functioning Iridium low-earth communications satellite, the imminent demise of safe space operations suddenly focused the UN's attention. If it had only stopped there, the space debris issue would be treated in the UN's typically ponderous but nonetheless predictable manner. This was exhibited at the June 2016 UNCOPOUS meeting where delegations managed to adopt a portion of the guidelines being drafted and discussed by its Working Group on Long Range Sustainability (LTS).[21]

The first "New Space" communications system may be OneWeb, which addressed an ITU confab on satellites and the information society on June 7th in Geneva.[22] OneWeb plans to launch 648 satellites by 2020, configured into 18 orbital planes orbiting at an altitude of 1200 km, communicating through potentially millions of earth-bound routers in the Ku and Ka-bands. The lower orbital height reduces the required power levels of both satellites and ground terminals, plus a reduced latency for round-trip signal paths as compared to the half-second delays with the much higher geostationary links at 35,000 kilometers. OneWeb is not alone. Amazon's Jeff Bezos and Facebook's Mark Zuckerberg also have plans for their own large constellations of small low earth orbit satellites bringing their flavors of Internet content directly to billions of future developing country and rural Internet customers. And you can bet that Google is not going to be left out of the LEO party. All told, even if only some of these systems actually get the

20 Federal Communications Commission (FCC), "In the Matter of Teledesic LLC: Application for Authority to Construct, Launch, and Operate a Ka-band Satellite System in the Fixed-Satellite Service," Source: http://personal.ee.surrey.ac.uk/Personal/L.Wood/constellations/fcc-teledesic.pdf (accessed July 21, 2016).

21 Author's notes.

22 "New space" is a term referring to the entrepreneurial firms of the 21st Century seeking to expand space utilization through tight public-private partnerships. See, Carren Jao, "Meet the Entrepreneurs at the Forefront of the Space Race," *Entrepreneur*, October 16, 2014. Source: https://www.entrepreneur.com/article/237409 (accessed on July 28, 2016).

funding necessary, within a few years literally thousands of small satellites, both alive and dead, will be orbiting a few hundred kilometers overhead. The potential benefit to bring broadband Internet to billions of developing country and rural users is significant but so too is the problem with space trash.

Advances in commercial "New Space" satellite and launcher technologies (witness Elon Musk's SpaceX's booster rocket landings follow launch) have perhaps made such large constellations feasible following the deployments in the 1990s of the Iridium and Globalstar non-geostationary systems. But with thousands of satellites, all with limited engineering lifetimes, the probability is high that a sizeable number will inevitably fail, become inoperable either in orbit, or fail to automatically de-orbit themselves as promised by the network operators. Thus we have a collision in orbit between the commercially-driven new entrepreneurs who want to take advantage of the miniaturizing technologies and the larger collective good of preserving orbital regions clean of space debris.

2.3.2. Electromagnetic Threats

Cyber industries are upsetting the conventional space governance applecart, especially in terms of electromagnetic security. For one, the cyber sector is financially huge, much larger than space. NASA's current budget is about $19 billion. Last year, Facebook spent reportedly $22 billion just to buy WhatsApp. Recently, Apple reported its first market downturn in 13 years; it still earned profits more than NASA's entire yearly budget. To paraphrase, one could today observe that 'cyber wags the space dog.' Now cyber giants Google, Facebook, Amazon, and their ilk are about to bulldoze a whole new space topography by launching thousands of small satellites into low earth orbits to bring the Internet from space directly 'to a smartphone near you, hackers and all.'

The bifurcated ITU-UNCOPUOS regime's attention is shifting from its long-standing focus on the geostationary satellites which are big and relatively few in number and operated by big governmentally-linked operators, to the much smaller and numerous commercially deployed entrepreneurial systems commonly called "New Space." And here is where the policy process is proving to be very sticky with great amounts of governmental inertia slowing the shift to a new set of "rules of the road" for the nimble space-Internet entrepreneurs.

Perhaps the most pressing problem threatening the operation and future of the Internet is cyber-conflict, intrinsic to all digital technologies. For wireless networks such as satellites, cyber-conflict was during the analog era confined chiefly to "jamming." Jamming, or intentional harmful interference (IHI), disrupts the communication pathway through transmission of a strong electromagnetic signal that (1) blocks the earthbound receiver's ability to capture the intended satellite signal, or, (2) blocks the satellite receiver's

ability to receive and re-transmit the intended signal back to earthbound receivers. IHI is illegal under ITU Radio Regulations and the ITU Constitution.[23]

As reported at the June 2016 ITU symposium on satellite interference issues, IHI is also on the wane.[24] Digital signal processing techniques enables satellite receivers to discriminate between desired and jamming signals. Improved signal forensics can quickly identify the IHI perpetrator, as well as equipment with embedded signal identifiers. As older generations of analog satellites are retired and placed in graveyard orbits, the IHI threat may significantly diminish further. Moreover, better training and certification of earth station operators will avoid many instances due to incompetent personnel. However, the electromagnetic vulnerability of new generations of digital satellites to malicious software hacking in all orbits is growing.

Jason Fritz, in his 2013 article, "Satellite Hacking: A Guide for the Perplexed,"[25] categorizes four kinds of malicious hacking:

> "Satellite hacking can be broken down into four main types: Jam, Eavesdrop, Hijack, and Control. Jamming is flooding or overpowering a signal, transmitter, or receiver, so that the legitimate transmission cannot reach its destination. In some ways this is comparable to a DDoS [Denial of Service] attack on the Internet, but using wireless radio waves in the uplink/downlink portion of a satellite network. Eavesdropping on a transmission allows a hacker to see and hear what is being transmitted. Hijacking is the unauthorized use of a satellite for transmission, or seizing control of a signal such as a broadcast and replacing it with another. Files sent via satellite Internet can be copied and altered (spoofed) in transit. The copying of files is eavesdropping, while spoofing them is hijacking, even though the access point and skillset used for file spoofing fits better with eavesdropping. This illustrates the ability, in some cases, for hackers to move seamlessly between categories, and the difficulty of placing strict categorization on types of satellite hacking. Controlling refers to taking control of part or all of the TT&C ground station, bus, and/or payload – in particular, being able to manoeuvre a satellite in orbit."[26]

The actual vulnerability was evidenced by alleged hacking originating from Russian territory of a US-German research satellite, "ROSAT," in 1998 rendering it useless after commanding its ultra-sensitive sensor to point to the

23 International Telecommunication Union, cite Constitution and RR.

24 Author's notes, ITU International Satellite Symposium 2016: *Interference-Free Satellite Frequency Spectrum – Myth or Reality?* June 13-14, 2016, Geneva, Switzerland.

25 See, Jason Fritz, "Satellite Hacking: A Guide for the Perplexed," Culture Mandala: Bulletin of the Centre for East-West Cultural and Economic Studies, Vol. 10, No. 1, December 2012 – May 2013, pp. 21-50. Source: http://www.international-relations.com/CM2012/Satellite-Hacking.pdf (accessed August 5, 2016).

26 Fritz, p. 34.

sun.[27] On August 16, 2016, China successfully launched "Micius" satellite, an experimental testbed for using quantum encryption employing principles of photon entanglement derived from quantum theory.[28]

3. Concluding Observations: Digital Governance of Outer Space

The proposed constellations of hundreds of low-earth orbit satellites for provision of Internet connectivity to potentially billions of users poses direct challenges to existing legal procedures and precedents for outer space governance in general, and cyber-conflict in particular. First, as discussed above, such constellations are organized around digital network architectures. The Internet's packet-switched digital architecture is intrinsically de-centralized in administration and control, but highly susceptible to unauthorized use and hacking. Thus any satellite system so intimately integrated into Internet infrastructures would itself be highly vulnerable to network disruptions. The analog era division between the satellite communications payload and the satellite's engineering platform no longer exists, creating the potential cross-hacking now evident for example in automobiles and perhaps even aircraft. Secondly, large low-earth orbital constellations will seek to use spectrum being used and sought by terrestrial digital mobile and geostationary satellite network providers. The engineering complexity and inevitable failures among hundreds of small satellites makes spectrum conflicts inevitable. Thirdly, the large constellations pose a significant vulnerability in terms of space debris and as a target for malicious hacking and IHI. In sum, the ITU-UNCOPUOS dichotomous "hard law" outer space regime will increasingly be absorbed into a system of "soft law" governance currently being developed by the Internet community.

3.1. The Commons Model for Outer Space Governance

The "flat" and open access structure for the multi-stakeholder Internet community has proved highly resilient to traditional "hard law" governmental efforts to subsume it within an enclosing traditional institutional structure consisting of governments and their authorized network providers.[29] Instead, the ITU itself has become much more oriented to a more open multi-stakeholder organizational structure. The UNCOPUOS has also inched towards a more open organizational architecture. Meanwhile,

27 Fritz, p. 39.

28 See, *Techcrunch*, "China launches the first quantum communications satellite – what is that exactly?" Source: https://techcrunch.com/2016/08/16/china-launches-the-first-quantum-communications-satellite-and-what-is-that-exactly/ (accessed August 17, 2016).

29 See, Jeremy Rifkin (2014) *The Zero Marginal Cost Society*, p. 196.

its June 2016 meeting set out a process for promulgation of Long Term Sustainability guidelines on a purely voluntary basis, most significantly for the issues of space militarization, space debris, and cyber-conflict.
According to economist Jeremy Rifkin, the world is only now beginning to realize the depth and breadth of the paradigm shift transforming governance brought on by the information revolution.[30] The hard shell of the traditional Westphalian sovereignty model of the nation-state fits neatly with hard law versions of top-down treaty governance. Analog networks were dominated by governmental monopolists and these were replicated in outer space. Technology is moving towards self-organizing intelligent "mesh" networks imbued by their creators with increasingly sophisticated levels of intelligence for self-management. What is needed is transparency in order to ensure security. As large constellation satellite networks take on ever greater attributes of shared mesh network configurations, governance will likewise shift, in Rifkin's words, towards a "collaborative commons."

3.1.1. Future Commons Directions: ICANN, Space Data Association, Internet of Things

The desired ubiquity of Internet connections required for modern commerce and communications is already driving business models towards an increasingly diversified range of satellite infrastructures and large constellations in GSO, MEO, and LEO orbital regions for customized provision of Internet connectivity. The Space-based Internet includes these proposed systems:

1. "OneWeb – Richard Branson's Virgin Group – Qualcomm – formerly WorldVu, has ITU authorization for Ku-Band at 1,200 km. for planned 648 satellites.
2. Elon Musk announced on January 16, 2015 SpaceX's plan for a network composed of 4026 satellites orbiting at 1,100 kilometer altitudes, financed with Google and Fidelity backing."[31]

The sheer financial clout of the Internet sector will increasingly come to dominate discussions over outer space governance as they relate to hacking, spectrum, debris, and interference issues. The key conclusion is that outer space governance will be increasingly dominated by factors originating in the cyber sphere with a very different legal heritage. As a result, outer space governance *in toto* will in coming decades come to resemble current Internet governance characterized by voluntary, non-binding agreements that mirror market dynamics. The over-riding concern of the firms dominating the Internet sphere both as suppliers and users now focuses on cyber-security

30 See, Rifkin, pp. 19-21.
31 See, Peter b. de Selding, "Enough satellites to darken the skies," *SpaceNews*, November 21, 2016, p. 30.

which will concomitantly dominate the dialogue over future directions of outer space governance. What will that outer space regime look like?
The Space Data Association (SDA) exemplifies the flat and voluntary organizational response to governance of space debris. As a non-governmental organization, the SDA serves as a clearinghouse for information about orbital objects, their trajectories, and possible collision threats. It relies on orbital parameters voluntarily supplied to it by its members about their launches and orbital operations. Proprietary information about satellite operations is anonymized, while making it possible to forecast and detect actual collision threats. Similar directions in Internet governance are taking hold as cyber-vulnerabilities of Internet-connected networks and appliances provide a widening diversity of targets to hackers.