IISL-97-4.17

SPACE TELECOMMUNICATIONS AND THE INTERNET: IMPLICATIONS FOR THE OUTER SPACE TREATY

Larry F. Martinez, Ph.D.*/
Department of Political Science
California State University
Long Beach, CA 90840-4605 USA
http://www.csulb.edu/~martinez

Paper Submitted to the
40th IISL Colloquium
Torino, Italy October 6-10, 1997

Abstract

The speedily expanding Internet is in the process of transforming the technological, economic, and policy bases for nation-state regulation of telecommunications, including space-based satellite networks. Deployment of the packet-switched Internet has accelerated the liberalization of telecommunications markets and has led to far-reaching regulatory restructuring and policy shifts regarding state ownership and control of networks and information flows. As space-based GMPCS networks become integral parts of the globalizing Internet infrastructure, the state-centric legal paradigm requiring state "authorization and continuing supervision" of space activities by "non-governmental entities" stipulated under Article VI of the OST and associated treaties forming the outer space legal regime will be called increasingly into question.[1] This paper examines the technological, economic/trade, and security issues that question whether the existing state-centric paradigm for regulating Internet-based GMPCS satellite systems will remain in legal phase with emerging liberalized regulatory regimes for terrestrial Internet-based infrastructures.

Introduction

Two milestones in the liberalization of world telecommunications markets have been passed during the last twelve months with far-reaching implications for international space law. In October 1996, the ITU's World Telecommunications Policy Forum adopted the principles for a Memorandum of Understanding (MOU) facilitating the use and transport of Global Mobile Personal Communications by Satellite (GMPCS) satellite terminal handsets over national borders. Among the GMPCS systems being deployed are those which will extend the Internet into low-earth orbit constellations of satellites which will interconnect seamlessly with the terrestrial Internet. In February 1997, the World Trade Organization concluded agreements liberalizing significant sectors of world telecommunications markets, providing an additional impetus for an even speedier expansion of the Internet. These

---

*/

set the stage for worldwide deployment of the Internet while eroding the technological, economic, and political foundations underlying the legal framework for nation-state regulation of low-earth orbit satellite communications. The goal of this paper is to stimulate discussion of the challenges Internet-based GMPCS systems pose to the Outer Space Treaty's (OST) state-centric legal regime for satellite communications, especially as it pertains to the Article VI assignment of state "authorization and continuing supervision."[2]

- **Technology Factors: Internet-based GMPCS satellite network architectures make compliance with OST Article VI stipulations for state "authorization and continuing supervision" increasingly difficult.**

System Architecture of the Internet (Network of Networks)[3]

Technology is the flipside of infrastructure economics and regulation. International law, originating during eras of agricultural and industrial primacy, acknowledged the state's preeminent legal status to control its technological infrastructure (postal services, telegraph, telephone and spectrum-based broadcasting and wireless telecommunications networks) as essential elements of state sovereignty and later, economic necessity. The parameters of state-centric international law congruently matched the technological and jurisdictional boundaries of governmental monopolists and their licensed natural monopoly infrastructures as evidenced in the OST and conventions governing the International Telecommunication Union (ITU) and other intergovernmental organizations focusing on state monopolist infrastructures (i.e., postal services, broadcasting, airlines, etc.).

This "natural monopoly" jurisdictional congruence is most clearly seen in the system architectures of geostationary satellite systems (GEOs) during the early decades of their development. GEO systems required massive front-end investments in multi-million dollar antennas, satellites, and associated equipment with the technical constraints inherent with *analog* signal processing technology (propagation, modulation, and channel access) which resulted in satellite networks operating essentially as "cables in the sky," network configurations that closely resembled existing terrestrial and submarine cable infrastructures and their concomitant natural monopoly regulatory regimes.

On a deeper technological level of analysis, analog signal processing requires the network operator to provide a discrete signal pathway (i.e., a circuit) for each pair or set of communicators. Control rested with the network provider who performed the circuit switching function within a circuit-based regulatory regime. Compliance with the OST Article VI stipulation requiring state "authorization and continuing supervision" of space-based GEO satellite circuits was straightforward as the state and the government monopolist network operator were in most cases the same entity and closely matched the network architecture. This was to radically change with the advent of digital signal processing techniques, most notable of which was the innovative packet-switched network architecture which has eroded the natural monopoly characteristics of telecommunications networks in general, and satellite communications in particular.

The Internet is a Packet-Switched Network

The origins and functioning of the Internet are shrouded in the near-myth-like veils of its Cold War inspiration, leading to the widespread belief the Internet works because it was designed to survive nuclear war. In 1964, California-based RAND Corporation researcher Paul Baran and British researcher Donald Davies independently conceived of a rather surprising solution to the military's problem of network survivability: assume that each signal's pathway would fail and build accordingly. The Baran-Davies' brainstorms split each message into sequentially numbered blocks (which Davies called *packets*), each of which would have an electronic address label slapped on by the sending computer and sent on their way. The sending computer would transmit each packet down the next available empty circuit, whereupon the packet would bounce from computer to computer using otherwise empty pathways until arriving at the destination computer. The receiving computer would then use the sequential address labels to reassemble the packets back into the original message. If message packets were missing or damaged because of pathway breakdowns, it would be a relatively simple matter to have the sending computer retransmit those packets using an alternative roadmap to the destination. [4]

The *digital* packet-switching proposal was blasphemous to the entrenched circuit-based theology rooted in the orthodoxy required by slow *analog* mechanical telephone switching centers that were geared to human conversations, not computer data bursts. The packet-switching thesis was Copernican in its eventual effect on the development of computers, far beyond its nuclear war inspiration of system survivability. Because a packet-switching system by design used whichever circuit was empty at the time a packet's transmission between computers, it achieved far higher communication efficiencies and economies to the great efficiency and cost benefit of the computer users. By sharing computer resources across a packet-switched network, they could get more work done, more quickly and efficiently. The economic and technological basis for state-operated natural monopolies has quickly eroded in the face of the Internet's explosive growth.

Analog to Digital: Convergence and Boundary Blurring

The Internet represents a major milestone in the transition from an analog-based telecommunications infrastructure to its digital successor. The vulnerability of analog transmissions to interference from unwanted electrical signals, required discrete communications pathways; hence, telephone, radio and television developed within well-defined technological and jurisdictional boundaries. *In the analog world, control rested with the network operator.* In earlier analog eras, a governmental regulatory authority ensured that a nation's telephone switches would interconnect two users with an interference-free (often "physical") synchronous electronic circuit between their telephone instruments. In contrast to analog network architectures, the Internet's digital packet-switched network architecture puts telephone, radio, and television on the same digital pipe, encoded onto data packets which are sent everywhere at the same time. Most significantly, in the asynchronous packet-switched Internet environment, the network merges with the computer, and *control shifts to the user.*[5]

In essence, in the totally-digital Internet environment, the network become just another part of the computer's interface with another component; the "Internet" looks like a disk drive. "Closed" analog systems are becoming "open" or "transparent" digital systems where network control is dispersed among users of the network(s). In contrast to the conventional analog network, where the "smarts" of the

network resided inside the telephone central switch (and therefore with the monopolistic network operator), today's computer consumer operates an appliance that rivals or supercedes slower adapting military or governmental computer networks. For example, on March 20, 1997, National Public Radio reported that a computer consulting group in the San Francisco area had managed to "crack" the new digital cellular encryption codes using off-the-shelf Intel pentium-class processors.[6]

In sum, "the Internet model, rather than the older hierarchical model of the circuit-switched telephone system" is becoming the basis for the telecommunications infrastructure of the 21st Century. As the technology-mandated circuit boundaries between telephone, radio, and television disappear, so too does the politically-mandated regulatory justification for a monopolistic network provider.[7]

Observations: Internet-based GMPCS Technology and the OST

GMPCS, the next generation of communications satellites, is moving control over information flows one step further away from state purview. While Motorola's *Iridium* narrowband system is already being deployed in orbit, a great deal of attention is directed at Microsoft's *Teledesic* projects,[8] a proposal place more than 600 satellites into low earth orbits (LEO). Satellite Internet users construct their own networks with the click of a computer mouse, bypassing domestic telephone networks completely as they communicate voice, data, or video on the Internet, from anywhere to anywhere.[8] In short, a state's ability to fulfill the OST requirement for state responsibility and control is eroding fast as digital Internet packet-switched networks replace their earlier analog infrastructures. If pathways change according to the whims of a packet-switched network router, no one can define the network's boundaries at any point in time. Furthermore, users will not even be aware that they may be using a space-based communications pathway and that their use may be subject a wholly different legal regime. The Internet's packet switching technology and the GMPCS system architectures are obsoleting traditional analog-era state monopolists and the clear-cut congruence between the boundaries of their national networks and the grant of monopoly control by the state and recognized by the OST.

- **Economics/Trade Factors: Liberalization of world telecommunications markets and services is making state compliance with OST Article VI provisions increasingly problematical with respect to Internet-based GMPCS systems.**

States or their legally-licensed monopolists have operated railroads, postal systems, power grids, and telephone/broadcasting infrastructures for many decades. The market and the transactions for many of these services took place entirely within the territorial boundaries of the nation-state. Today, traditional arguments underlying these arrangement based upon economies of scope and scale are falling by the wayside as states privatize and liberalize large formerly public sectors. In addition, market transactions themselves are no longer taking place within the purview of the nation-state. The boundaries for what once was considered a domestic or foreign transactions are blurring owing to the massive flows of capital along global data networks. The Internet is already accelerating the shift of transactions for a growing range of services out of the territorial boundaries of states into an as yet unclaimed regions of cyberspace.

Privatization to Liberalization:

What is the appropriate role for the state? In this era of far-reaching alterations to both the physical and mental landscapes of what used to be familiar vistas toward the public good or political legitimacy, the issue of how or even whether governments should regulate the telecommunications/information sector is increasingly the subject of national and international debate. Two issues stand out: privatization and liberalization. *Privatization* is the process of transferring ownership of what were usually government-owned telephone and broadcast industries to private stockholders. The transfer of ownership may mean a transfer of investment, profit, and risk, but not an actual transfer of regulatory control. That may still lie with governmental ministries who may, by regulatory fiat, establish service areas, prices, and market structure. *Liberalization* refers to a reduction in government's jurisdictional competence in regulating what firms may or may not do within their allowed market or service areas. Hence, liberalization connotes a change in control and a lessened role for the state in both OST Article VI areas of authorization and continuing supervision.

Even in cases where there is some market access afforded competitors, the governmental monopolist as the initial or dominant provider benefits from the high entry costs new entrants must bear to install facilities to each home or business. Electrical power and natural gas distribution networks are generally operated as public utilities due to their natural monopoly characteristics. In these cases of natural monopoly, the public interest is promoted through authorization of a provider within a regulatory regime to monitor pricing and costing practices so that all users were able to access the network for essentially the same price regardless of the actual cost (i.e., universal service at uniform (equitable) pricing). Today, however, there is a growing acceptance that the natural monopoly argument against telecommunications privatization and/or liberalization was valid only for the economies of scope and scale present for *analog* technologies operating under conditions of network resource scarcity. As communications infrastructures shift to digital computerized networks, so-called channel scarcity and arguments for natural monopoly are falling as quickly as the prices for computing power.

Convergence

The analog world is one of channel scarcity owing to the discrete and different pathways each signal travels. As each new technology came into its new market, it used a different pathway to its users. Hence, telephones initially used a massive grid of wires and switches; radio and television an invisible set of pathways through the airwaves. In each case, to sustain the public good aspects of universal service at uniform prices, market entry was prohibited against potential "cream skimmers" who would otherwise attempt to take advantage of the natural monopolist's requirement to cross subsidize access for high cost users by charging rates significantly above actual costs to low cost users. Scarcity of channels, whether telephone lines or airwaves, reinforced the strictures of natural monopoly regulation to prevent market entry to potential cream-skimmers.[8]

Intergovernmental agreements establishing the de facto natural monopoly satellite networks owned and operated by state monopoly providers, such as INTELSAT or INMARSAT, could, in effect, ensure compliance with OST Article VI stipulations through monopoly protection mechanisms such as the INTELSAT Agreement Article XIV(d).[9] Legal scholar Carl Christol argued that the 1967 Outer Space Treaty and subsequent legal instruments "prevent juridical person, other than States - and in particular international intergovernmental organizations - from claiming

exclusive operational, as well as management rights, which are denied to States."[10] However, in the digital era states are attempting to claim control over computer information in its digital form, ones and zeros, which may well travel down the same network pipe, be it wire, fiber optic, terrestrial cells, or satellite - constituting a massive volume of services and information flows - that defy any attempt to block market entry *once the pipe is in place*.

The "social contract" between governmental network monopolists and users which required "authorization and continuing supervision" of entrants into a natural monopoly market has fallen to the tremendous market synergy between personal computers, computer networks, and market liberalization fueling the explosion of the Internet in the early 1990s, resulting in 1996 Telecommunications Reform Act.[11] Analogous (so to speak!) developments are taking place in growing numbers countries liberalizing their financial and communications infrastructures.

❑ Political Factors: National Security, Internet-based GMPCS, and Legal Boundaries

The 1990-91 Persian Gulf War fundamentally altered perceptions about the nature of warfare and national security in the information age. As Nye and Owens observe in a 1996 *Foreign Affairs* article:

> Knowledge, more than ever before, is power. The one country that can best lead the information revolution will be more powerful than any other.[12]

Many credit American information power prowess to its liberalized information and telecommunications regulatory structure. More than it being merely an "open society," profit motivations successfully inspired American data processing, telecommunications, and broadcasting firms to expand and diversify on an unprecedented scale. However, the race to commercialize cyberspace also raises a rather uncomfortable policy and legal issue: If information technology is today a key component of military strategic/tactical power, are states capable of complying with OST Article VI to ensure that competitive activities of commercial companies do not violate international legal precepts banning aggressive uses of power?

Case in point: In June 1996, Israel asked the United States Government to restrict U.S. commercial satellite firms operating remote sensing satellites with 3-meter resolution or better from imaging Israeli and neighboring territory.[13] Israel's request is indicative of the international legal and political issues coming to a boil as information technology makes territory and the international legal principles based on territory increasingly irrelevant. Moreover, the definition of aggressive war or illegal intervention may also be obsolete in cyberspace and hence for the OST-imposed obligations on states attempting to supervise GMPCS systems. Legal cyberscholar Sean Kanuck points out that

> There is a critical distinction between "Information Age warfare," which utilizes new technologies to transform the conduct of war while still pursuing traditional military objectives, and "Information Warfare," which redefines the very nature of international conflict. Information Warfare has officially been defined as follows: Action taken in support of national security strategy to seize and maintain a decisive advantage by attacking an

> adversary's information infrastructure through exploitation, denial, and influence, while protecting friendly information systems.[14]

Or alternatively as:

> Any action to deny, exploit, corrupt, or destroy the enemy's information and its functions; protecting ourselves against those actions; and exploiting our own military information functions.[15]

Kanuck writes:

> Thus, a tripartite legal distinction exists under international law. The first class of observational, data-collection activities are simply subject to domestic regulations. The second tier of activities, pro-active efforts to influence domestic affairs short of armed engagement, are most often violations of domestic law and are also "condemned" by international law. Finally, threats or actual use of force are expressly proscribed by the United Nations Charter as well as customary international law.[16]
>
> Therein lies the critical distinction behind both the future of international conflict and the latent deficiency of public international law. As information evolves into the target itself (i.e., its destruction becomes the veritable end, rather than a means to other military objectives), the entire concept of warfare will be revolutionized. [17]

Hence, what Kanuck is arguing in analogous to the evolution of regulatory structures, i.e., from circuit-based regulation to service-based regulation. A new paradigm of international law is needed to shift from outmoded principles based on territoriality (discreet analog circuits) to one based on the digital paradigm, i.e., services.

> Even the basic military-civilian distinction under the customary laws of war (*jus in bello*) was founded on the theoretical ability to segregate physically those two types of entities in order to determine what hostilities could be perpetrated on each category. Today, it is becoming increasingly difficult to separate fully the military and civilian networks because they utilize many of the same satellites, fiber optics, computer nodes, etc.[18]

Kanuck advocates a long look at the existing prohibitions against intervention in the domestic affairs of another state as the most promising field for developing a usable legal paradigm for cyberwar.

> Interactions, and not physical territory, must become the basis of the new system; only then can aggression and intervention be redefined in terms of undesired effects and not merely the direct or indirect use of armed forces.[19]

In sum, states' ability to comply with the Article VI stipulation requiring state "authorization and continuing supervision" of non-governmental (i.e., commercial) entities utilizing the Internet-based GMPCS may be inadequate in the light of encryption techniques that will further hide who is using a GMPCS system and to what purpose.

Conclusion: Role of the State

The emergence of Internet-based GMPCS communication satellite systems utilizing privately owned terrestrial gateway earth stations, easily transportable handsets, and Internet packet-switching technology, represent a quantum leap in the seemingly inexorable march toward a privately-owned commercial Global Information Infrastructure (GII). As voice, data, and broadcasting services migrate towards an Internet-based infrastructure, traditional governmental jurisdictional boundaries will blur further, making all the more visible the apparent inability or unwillingness of states to comply with the OST Article VI obligations. The OST, promulgated during an era of governmental space programs and telecommunications monopolies, is premised upon technological, economic, and security boundaries of state jurisdiction that may no longer exist.[20] Instead, a new paradigm for managing commons resources may be required that utilizes the self-organizing parameters of the emerging Internet paradigm for international cooperation.[21]

Notes:

1. Article VI of the OST states:
States Parties to the Treaty shall bear international responsibility for national activities in outer space, including the moon and other celestial bodies, whether such activities are carried on by governmental agencies or *by non-governmental entities*, and for assuring that national activities are carried out in conformity with the provisions set forth in the present Treaty. *The activities of non-governmental entities in outer space, ... shall require authorization and continuing supervision by the appropriate State Party to the Treaty....* [emphasis added]

Treaty on the Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and other Celestial Bodies, Jan. 27, 1967, 18 U.S.T. 2410, T.I.A.S. No. 6347, 610 U.N.T.S. 205 (effective Oct. 10, 1967) [hereinafter Outer Space Treaty]. The other four treaties treat the questions of space liability, registration of objects, rescue and return of objects and astronauts, and an agreement covering activities on the moon and other solar system celestial bodies: *Convention on International Liability for Damage Caused by Space Objects* (1972) , 24 U.S.T. 2389, T.I.A.S. 7762; The Agreement on the Rescue of Astronauts, the Return of Astronauts, and Objects Launched in Outer Space (1968), 19 U.S.T. 7570, T.I.A.S. 6599; *The Convention on the Registration of Objects Launched into Outer Space* (1976), 28 U.S.T. 695, T.I.A.S. 7762; *The Agreement Governing the Activities of States on the Moon and Other Celestial Bodies* (1979), United Nations General Assembly Resolution 34/68.

2. See, "Memorandum of Understanding on GMPCS now ready for signing - GMPCS continues to make history," *ITU News*, #3 1997, pp. 5-7. Commercialization of space activities has proceeded apace in the areas of space launch vehicles, space remote sensing, space navigation. "WTO's landmark agreement on basic telecommunication services," *ITU News*, #4, 1997, pp. 34-38. While this paper focuses on liberalization of space telecommunication sectors and the GMPCS in particular, readers are urged to refer to articles by Fred Kosmo Note: The Commercialization of Space: a Regulatory Scheme That Promotes Commercial Ventures And International Responsibility. 61 *S. Cal. L. Rev.* 1055 (May, 1988). Source: Nexis-Lexis; see also, Kunihiko Tatsuzawa, "Policy and Law in Space Commercialization," in K. Tatsuzawa (ed.) *Legal Aspects of Space Commercialization*, (Tokyo: CSP Japan, Inc., 1992), pp. 10-31.

3. An earlier version of this analysis was presented in a paper to the Southwest Social Science Association

Conference in New Orleans, March 1997, while a more complete description of the Internet's underlying technology can be found in an article written in 1996 for the United States Information Administration.

4. See, Katie Hafner and Matthew Lyon, *Where Wizards Stay Up Late: The Origins of the Internet,* (New York: Simon and Schuster, 1996), pp. 53-65.

5. See, Richard Jay Solomon, "Telecommunications Technology for the Twenty-first Century," in William J. Drake (ed.), *The New Information Infrastructure: Strategies for U.S. Policy,* (Washington, DC: A Twentieth Century Fund Book), pp. 93-111; also,"GMPCS: The Regulatory Dilemma, ITU, World Telecommunications Policy Forum pamphlet, 21-23 October 1996. Teledesic Web Page: http://www.itu.int/pforum/paper2-e.htm

6. Author's notes from *National Public Radio* "All Things Considered" news broadcast on March, 20, 1997.

7. See, Revised *Report by the Secretary-General: Policy and Regulatory Issues Raised by Global Mobile Personal Communications By Satellite (GMPCS),* International Telecommunication Union, October 23, 1996.

8. See, Gregg Daffner and Larry Martinez, "The Legal And Economic Dimensions of A Competitive Global Satellite Regime: Consequences for Developing Countries," paper presented to the International Bar Association Conference, New York, NY, in October 1990.

9. *INTELSAT Agreement*, Article XIV (d).

10. Quoted from Glenn H. Reynolds and Robert P. Merges, *Outer Space: Problems of Law and Policy,* (Boulder: Westview Press, 1989), pp. 80-81.

11. The official citation for the Act is: *Telecommunications Act of 1996,* Pub. L. No. 104-104, 110 Stat. 56 (1996).

12. See, Eliot A. Cohen, "A Revolution in Warfare," *Foreign Affairs*, March-April 1996, pp. 37-54.

13. Warren Ferster, Israel Wants Imagery Ban, *Space News*, June 17-23, 1996, p. 1.

14. Sean P. Kanuck, Information Warfare: New Challenges for Public International Law, 37 *Harv. Int'l L.J.* 272 (Winter 1996). Fn. 7, citing the U.S. Office of the Chief of Naval Operations, Dep't of the Navy, Opnavinst 3430.26 1 (Jan. 18, 1995). Source: Nexis-Lexis.

15. *Id.*, fn. 9, citing the U.S. Dep't of the Air Force, *Cornerstones of Information Warfare* 3--4 (1995). Source: Nexis-Lexis.

16. *Id.* p. 276; fn. 19: "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any manner inconsistent with the Purposes of the United Nations." *U.N. Charter,* Article. 2, para. 4.

17. *Id.*, p. 286.

19. *Id.*, p. 292.

20. See, Brian Kahin and Charles Nesson, *Borders in Cyberspace*, (Cambridge: MIT Press, 1997).

21. Anthony Rutkowski, "The Internet: An Abstraction in Chaos," in *The Internet as Paradigm,* monograph published by the Aspen Institute, 1997, pp. 1-22.