IISL.1.-94-822

The Outer Space Cyberspace Nexus: Satellite Crimes

Michael Potter*
Director Esprit Telecom
Amsterdam

Abstract

This paper provides an analytical framework for understanding the intersection of cyberspace and outer space. By utilizing this framework we can better understand the anatomy of satellite crimes. The framework can facilitate answers to such questions as to whether a crime took place, what jurisdiction is likely to be involved, and what parties may be victims to the crime. This paper is intended to raise a number of legal and policy issues. The paper concludes that as cyberspace and outer space become increasingly internationalized there will probably be a need for more law created to govern and enforce satellite crimes.

I. Introduction

The purpose of this paper is to explore the expansion and collision of the two modern frontiers-- outer space and cyberspace. Nobody can say exactly what each of these frontiers is, where they begin, where they end, or even what these frontiers mean to mankind. It is almost certain that decades, even centuries from now experts will continue to wrestle with variations of the issues that have recently begun to challenge us.

*** Director of the Global Telecommunications Society, Member of IISL.**

This paper is particularly relevant to the theme of this conference: "Space and Cooperation for Tomorrow's World." While cyberspace and satellite crimes are recent phenomena, by better understanding these emerging issues we can come closer to addressing the moral challenge presented by this conference theme.

In an effort to tie the themes of this paper to our presence here in Jerusalem, a stunning religious capital, of at least three of the world's great religions, I will quote from Cyberspace: First Steps:

> ...the earthly *garden* Eden (and even to that walled garden, Paradise) then, floats the image of the Heavenly City, the new Jerusalem of the book of Revelation. Like a bejeweled, weightless palace it comes down out of heaven itself 'its radiance like a most rare jewel, like a jasper, transparent' (Revelation, 21:9). ...In fact, all images of the Heavenly City--East and West--have common features: weightlessness, radiance, numerological complexity, palaces upon palaces, peace and harmony through rule by the good and wise, utter cleanliness,

> transcendence of nature and of crude beginnings, the availability of all things pleasurable and cultured...Thus, while the biblical Eden may be imaginary, the Heavenly City is doubly imaginary: once, in the conventional sense, because it is not actual, because it *is* information, it could come into existence only as a virtual reality, which is to say, fully, only 'in the imagination.'...And a religious vision of cyberspace.[1]

Since billions of people for millennia have pursued religion in the hopes of grasping heavenly paradise, the quoted text above raises issues of enormous magnitude. Can we better understand the elusiveness of heavenly paradise by better understanding cyberspace? Can we come closer to heavenly paradise by coming closer to cyberspace?

And cyberspace has already arrived in this region of the world. In a recent article in The Jerusalem Post entitled "Hooked on Internet," the writer pointed out:

> Hours before Israelis would read the text of their agreement [March 31, 1994 Israel-PLO agreement] in their newspapers, diplomacy mavens around the world were pulling the detailed document straight out of the Israel Information Service, located in the Foreign Ministry's computer, using Internet, the worldwide link of computer networks.[2]

In more concretely ways today's satellites, which are part of the cyberspace infrastructure are transforming entire cultures. Programming such as MTV and Baywatch (the most widely watched T.V. program in the world) are having profound and lasting effects. To paraphrase Joseph Stalin, some may ponder how many military divisions is equivalent to the power of a satellite.[3]

Presently, space law has a conspicuous vacuum in this fast moving field. Following, I provide a framework which is intended to improve our understanding and ability to analyze the intersection of outer space, cyberspace and law.

The framework that will be elaborated later in this paper consists of the following conceptual categories which are intended to assist in providing a comprehensive approach to tackling the difficult issues that arise from the collision of outer space and cyberspace:

1. Origination
2. Transportation
3. Termination
4. Content

There are other conceptual constructs that one could propose for understanding satellite crimes. For instance the rather simple binary category of victims and perpetrators or a slightly more developed framework of input, processing, and output could be imagined. However, the framework that I present attempts to capture the entire communications process. If a crime takes place it should take place somewhere on the continuum in which this framework is presented. By understanding where it takes place in the process we can then consider the

legal and policy issues that may arise from such a crime.

Before discussing these four categories, it is necessary to explore the notion of cyberspace.

II. Defining Cyberspace

What is cyberspace? One might think that a logical approach to searching for this meaning would be to go on-line and check the encyclopedia. According to the CompuServe encyclopedia, cyberspace is defined as:

> Researchers in computer-imaging technology are trying to develop systems that will enable observers to experience a simulated three-dimensional reality. This simulated reality is known as virtual reality (VR), or cyberspace.
>
> Technologists since the 1970s have learned how to produce animated computer images of objects that exhibit the colors, textures, and changing spatial orientations that their counterparts exhibit in the real world. The images can also be subjected to changing light conditions and to simulated effects of gravity and other forces. The results can look as real as actual motion pictures. The further aim is to "enter" and actually manipulate VR, or cyberspace. Thus far this is done by having an observer wear a large complex headgear through which computer images are fed to small screens in front of the eyes, while gloves or full suits equipped with networks of sensors transmit apparent changes of body orientation in VR. (A simpler form of VR is seen in the flight simulators used for training military pilots.) Advanced VR systems can also provide three-dimensional sound. Potential uses of VR range from the long-distance manipulation of robot devices to the retraining of stroke victims in the use of their limbs.[4]

However, this definition is hardly satisfactory. Cyberspace: First Steps provides the following more convincing definitions:

> Cyberspace: A new universe, a parallel universe created and sustained by the world's computers and communications lines. A world in which the global traffic of knowledge, secrets, measurements, indicators, entertainment, and alter-human agency takes on form: sights, sounds, presences never seen on the surface of the earth blossoming in vast electronic night.
>
> Cyberspace: Accessed through any computer linked into the system; a place, one place, limitless; entered equally from a basement in Vancouver, a boat in Port-au-Prince, a cab in New York, a garage in Texas City, an apartment in Rome, an office in Hong Kong, a bar in Kyoto, a cafe in Kinshasa, a laboratory on the moon.

> Cyberspace: The tablet become a page become a screen become a world, a virtual world. Everywhere and nowhere, a place where nothing is forgotten and yet everything changes.[5]

I cannot improve on the poignant definitions provided above. However, for the purposes of this paper it is important to clarify that when I am talking about cyberspace, I am referring to the process of transmitting, receiving, storing and manipulating information through telecommunications.

Cyberspace itself is simply a higher level of evolution directly linked to the printing revolution. Again to tie our presence in Jerusalem to this subject it is worth noting that the technology which produced the bible allowed for a transportability of ideas, language, culture, and religion which make this city so important to so many people.

> ...first, with the development of writing, counting and modes of graphic representation, and then, centuries later, with the invention of the printing press and the spread of literacy of ephemeral communications came to be recorded at an unprecedented scale. More important for our story, these "records" came to be easily duplicable, transportable, and broadcastable.
>
> Life would never be the same. The implications of the print revolution and the establishment of what Marshall McLuhan called the "Gutenberg Galaxy" (in his book with the same name) for the structure and function of technologically advancing societies can hardly be overestimated. Not the least of these implications were (1) the steady, de facto, democratization of the means of idea production and dissemination, (2) the exponential growth of that objective body of scientific knowledge, diverse cultural practices, dreams, arguments, and documented histories...[6]

It is interesting to note that some experts have attributed the growth of religious fundamentalism to electronic mediums. Their argument is that, "Whereas print isolates individuals, sponsoring rational, dispassionate analysis, spoken words encourage group-thinking, sometimes mob-thinking."[7]

Previously I have sought to establish a working definition for the term cyberspace. Next I will clarify the relationship between cyberspace and outer space.

III. The Cyberspace Outer Space Nexus

There are two intersections between cyberspace and outer space. The first is a conceptual intersection and the second involves applications in the area of satellite communications.

A. The Conceptual Intersection of Cyberspace and Outer Space

It may be helpful to start with a definition of outer space. According to the CompuServe encyclopedia outer space is defined as:

> (1) Any region of space beyond limits determined with reference to the boundaries of a celestial body or system, especially: (a) The region of space immediately beyond Earth's atmosphere. (b) Interplanetary or interstellar space.

The first observation is that both cyberspace and outer space are two of perhaps the most important frontiers that mankind can embark upon. There are fundamental definitional and legal problems with both of these frontiers: Where do they begin? Where do they end? Whose jurisdiction is relevant in these domains? Can crimes be committed in these frontiers? Metaphysical notions of time and boundaries are raised by both frontiers. While philosophers and legal experts have discussed the implications of mankind living and working in space in a more permanent and widespread way than exists today, at this moment a substantial sub-culture is working, exploring, being entertained and communicating in cyberspace. One writer has argued:

> ...this should not mask the power of the implicit notion that *space itself* is something not necessarily physical: rather that it is a 'field of play' for all information, only one of whose manifestations is the gravitational and electromagnetic field of play that we live in, and that we call the real world. Perhaps no examples are more vivid than the beautiful forms that emerge from simple recursive equations--the new science of 'fractals'--and recent discoveries of 'strange attractors,' objects of coherent geometry and behavior that 'exist' only in mathematical spaces (coordinate systems with specially chosen coordinates) and that economically map/describe/prescribe the behavior of complex, chaotic, physical systems. Which reality is the primary one? we might fairly ask.
>
> Actually, why choose?
>
> Modern physicists are sanguine: Minkowski had shown the utility of mapping time together with space, Hamiltonian mechanics lent themselves beautifully to visualizing the dynamics of a physical system in n-dimensional *state* or *phase space* where a single point represents the entire state of the system, and quantum mechanics seems to play itself out in the geometrical behavior of vectors in *Hilbet space,* in which one or more of the coordinates are 'imaginary'.[8]

The quote above suggests the conceptual similarity between the two frontiers of cyberspace and outer space. While the conceptual parallels may theoretically be clear and compelling, the intersection of satellite applications and cyberspace is perhaps more tangible.

B. The Tangible Intersection of Cyberspace and Outer Space: Satellites

As described above cyberspace involves the use of telecommunications to transmit and receive information. A substantial portion of telecommunications involving cyberspace is in fact terrestrial. However, in this paper I am more interested in that portion of cyberspace that involves the use of satellite telecommunications facilities. What happens when cyberspace collides with outer space? Cyberspace is a neutral phenomenon--it can facilitate either good or evil. What happens when a satellite is used in an unauthorized fashion? Who is responsible? Who should pay? Did a crime take place? What laws were broken? Whose jurisdiction is relevant?

In order to better comprehend these difficult issues I put forward a framework which is intended to provide a better understanding of where an illegal activity takes place when we are concerned with the cyberspace outer space nexus.

IV. A Comprehensive Framework for Understanding the Intersection of Outer space, Cyberspace

The four stages of the continuum are intended to provide a general framework for illuminating the intersection of outer space and cyberspace. This framework can help us determine where the intersection of cyberspace and outer space takes place, and whether an event violates local laws or international space law as well as identify some of the larger technological and policy issues.

A. Origination

This is the process in which a message or a program is transmitted. Origination is generally associated with a carrier or broadcaster that is sending information on behalf of a third party customer or on a first party basis. There are two categories of origination that warrant consideration: hardware issues and data related issues.

1. Data Related Origination

Perhaps the most obvious question that arises is whether the broadcaster or carrier is properly licensed. For example questions were recently raised when the Polish authorities closed six local stations that were unlicensed. Under the new Polish broadcast legislation, broadcasters could not have more than 33 percent of their equity owned by foreigners.[9] There is the famous case of the Home Dish Satellite (HDS), broadcaster of a number of pornographic channels including Exxxtasy, which was attacked by enthusiastic American prosecutors. The prosecutors even went after the satellite carriers who had no direct connection with the offensive programming. GTE Spacenet, and U.S. Satellite Inc., were apparently surprised when an Alabama grand jury included the companies as defendants in a 504-count criminal indictment.[10] A GTE spokesperson responded to the charges by stating: "As a communications common carrier regulated by the Federal

Communications Commission, GTE Spacenet has no authority to censor what customers use our satellites to transmit."[11]

Since 1988 it has been illegal to broadcast pornography under federal laws in the U.S.[12] However, it has been argued that pornography that originates from outside the country to viewers in the U.S. by satellite does not violate U.S. law.[13] While the U.S. is party to the international treaty for The Repression of the Circulation of Obscene Publications, it would be unlikely that such a treaty would have impact over an international commercial provider.[14]

The Indian government has been fighting with Pakistan over the use of satellite television. India has accused Pakistan of using World Bank Funds to rent a satellite transponder for the purpose of broadcasting propaganda into India.[15] Unwelcome satellite programming arriving into sovereign territory has generated enormous amounts of controversy and books have been written on this subject.[16] In fact, India in the past has banned the broadcast of jewelry and baby food advertisements on T.V. because the government is worried that viewers will be overwhelmed with greed.[17] In the U.S., female employees of Strogh Brewery filed a suit against the company for sexual harassment, discrimination and assault in the workplace for broadcasting its T.V. commercial featuring the Swedish Bikini Team.[18]

2. Hardware One of the problems that the International Maritime Satellite Organization (INMARSAT) has is that its analog terminals can be compromised ("hacked") so that the users of the modified terminals can effectively receive "free" phone calls.[19]

There are a many instances where the content/hardware issues overlap. For example, drug smugglers use the hacked INMARSAT terminals to carry-out criminal activities. In one interesting case an uplink for Playboy channel was interfered with by an individual who wanted to substitute the program of nudity for one of religion. The perpetrator was convicted of intentionally interfering with a communications satellite broadcast and operating a satellite uplink transmitter without authorization.[20]

B. Transportation

1. Transporting Data This term refers to the transportation of voice and content (data) through terrestrial and space links. When hackers (or phone phreakers) gain illegal access to the INMARSAT network their actions are not only limited to the origination side of the framework that I present here, but infringe on the transportation side of the framework.

Another transportation issue is spectrum piracy through the use of spread spectrum technology. There is extensive documentation on technical issues involving spread spectrum (a technology that efficiently uses small pieces of various available sections of the spectrum) , but almost no documentation about the current use of spread spectrum for satellite communications. Industry sources have explained that agencies like the U.S. Drug Enforcement Agency

(DEA) use spread spectrum to "share" or "piggy-back" on existing satellite infrastructure. This may not cause technical interference, but it has been reported that it consumes satellite power.[21] Certainly, one can question what the implications would be if a operator would commercially provide such services.

2. Transportation Related Infrastructure This is a broad category that warrants separate treatment in its own right. By infrastructure I am referring to the elements of satellite infrastructure that are not terrestrial oriented. This includes spectrum, orbital positioning and satellites.

Earlier this year the Chinese launched the Apstar-1 satellite which was illegally positioned too close to existing satellites. Japan accused China of violating regulations established by the International Telecommunications Union, a 182-country, United Nations-affiliated body that supervises the global use of satellite slots and frequencies.[22] Some experts suggest that the resolution of this problem, which is rumored to have been a cash settlement, sets a dangerous precedent. Another issue in this area involves the "black marketing" of orbital slots. These were the accusations made against the Kingdom of Tonga when they applied for prime orbital slots over the Pacific. Because the Kingdom of Tonga did not have a history of building, launching and operating satellites, there was speculation that this precious orbital real-estate would be resold to other parties. Some suggest that the Kingdom of Tonga has simply taken advantage of existing ITU rules.

In January of 1994, two Canadian Anik satellites were damaged. The Anik E-1 had temporary problems but was later restored. The Anik E-2 has never recovered. The official version from Telesat is that their satellites were hit by solar storm. However there are other explanations:

> ... international computer bulletin boards for satellite buffs and space experts were busy this week with speculation. Some were saying that computer hackers or disgruntled employees have sent "kill" messages to the satellite, or that an employee screwed up, or that Telesat skimped on protective shielding.[23]

If this speculation is correct about intentional damage this would be similar to a case in New Jersey where a hacker was accused of actually breaking into a satellite control center and moving a satellite. Satellite organizations are not keen to publicize these types of events. It can be argued that these types of activities involve both origination and transportation issues.

C. Termination

I will use the term termination interchangeably with reception. Termination is usually associated with voice telephony, while reception with broadcast satellite telecommunications.

Perhaps one of the most economically significant areas of satellite related crimes involves the use of unauthorized reception of T.V. broadcast. This is

often referred to as T.V. piracy. It is usually accomplished by the sale and the use of unauthorized decoder boxes, permitting users to view programming without paying subscription fees. In the U.K. two individuals were recently charged with conspiracy to defraud the Direct Broadcast Satellite (DBS) provider British Sky Broadcasting for the alleged sale of pirate decoding cards.[24] The Motion Picture Export Association of America is pressuring the EC to ban unauthorized decoders. Currently only the UK, Sweden, and France have passed such laws. In the U.K. it is illegal to knowingly make, import, sell or rent pirate decoders, but it is not illegal to own one.[25] Only one-fourth of the four million Television Receive Only (TVRO) dish owners are estimated to possess licensed descrambling equipment. The "mother" of all scramblers, the VideoCipher II Plus code, has apparently already been cracked by hackers according to the underground publication Satellite Watch News.[26]

The unauthorized monitoring of private communications is not permitted by ITU regulations. However, this practice is widespread. Monitoring can arguably fall between the areas of transportation and termination. The principle of the inviolability of telephone conversations is in fact guaranteed in the constitutions of several countries including Austria, Germany, Greece, The Netherlands, Portugal and Spain. The European Convention on Human Rights has been interpreted by the European Court of Human Rights as covering the secrecy of telephone conversations.[27] One can refer to available publications such as Monitoring Times where an entire article has been dedicated to instructing readers on how monitor INMARSAT phone calls.[28] Another article in the same magazine suggests that "monitoring orbiting satellites" is a "fascinating and educational facet of the radio monitoring hobby."[29] Additionally, U.S. legislation is being proposed that would force carriers to reengineer their networks so that law enforcement could more easily monitor phone calls.[30] An American businessman was convicted of attempting to deliver a satellite system to the government of Jordan that would have allowed them to monitor phone calls throughout the Middle East.[31]

Three hackers were accused of causing havoc with weather computers before the allied invasion into Iraq and were charged under the U.K. Computer Misuse Act. The action that they allegedly committed can arguably fall into the area of satellite data termination. Plans for Operation Desert Storm had to be radically altered, inadvertently jeopardizing, almost fatally, the effort against Saddam Hussein. The Cray computer they broke into was:

> ...playing a key part in the build-up to the war by providing the Allies with up-to-the minute weather predictions. The Cray which is capable of making 1,000 calculations a second, is not only linked to a chain of satellites circling the globe but also receives data from land-based meteorological sites and weather ships throughout the world.
>
> By breaking the codes and inserting their own data the amateur trio slowed down the

> split-second rate at which the computer received 'weather pictures' from the satellites in outer space. This action effectively threw the whole system out of synchronization and gave a totally inaccurate advance picture of the weather conditions expected in the Gulf region.
>
> The White House even threatened to withdraw European access to the international communications satellite which carries electronic and telephone traffic across the Atlantic if the hackers' activities were not curbed. [32]

It is worth noting that according to the INTELSAT charter its satellites are not to be used for non-peaceful purposes. Yet during the Gulf War, INTELSAT satellites were used for a wide variety of Allied military activities.

In the early 1970s, the U.S. Department of Defense (DOD) began investing an estimated $10 billion in a constellation of 24 communications satellites known as the Global Positioning System (GPS). The system allows military users to pinpoint their location using GPS equipment. Citing national security issues, DOD distorts the GPS signal to non-military users so that their location can be off by up to 300 feet. One of the reasons for this concern is that an enemy could use GPS as a guidance system for a missile or an aircraft. One way to get around this regulation is to use the Russian Glonass satellite system which has been hacked by western businessmen.[33]

D. Content

The area of content is one of the most debated areas of telecommunications. One of the most contentious content issues revolves around the issue or pornography. Pornography is not limited to satellite broadcast but also includes telephone numbers that when dialed involve the caller paying some form of fee (in the industry this is often referred to as audio text). Recently the Chairman of Belgacom was charged as co-responsible for inciting 'debauchery and prostitution' through leasing out sex lines.[34] Countries such as Guyana (where the phone system is largely connected internationally by satellite) are developing the reputation of creating entire audio text industries. "Gross revenues to telcos from international audiotext services approached US $900 million in 1993, a market size comparable to the European domestic audiotext market. Traffic volumes were between 600-750 million call minutes and the service providers' share almost US $250 million."[35] According to a recent article:

> The future of international [audio text] services rests ultimately with bodies such as the International Telecommunications Union (ITU). A body which is responsible for regulating international telecommunications traffic, and is now having to face up to the problems of considering the content of services rather than just the carrier aspects.

> It would seem logical that value-added services should be subject to the local regulations of the country where the service is advertised. However, the ITU is a United Nations agency and operated on the principle of one member one vote. The 184 members of the ITU are national telecommunications administrations. Although Surinam has essentially the same voting power as the US, the prospects for future legislation remain unclear."[36]

The indictment against Home Dish Satellite for the national distribution of obscene matter by satellite was the first major test case of federal and state laws in this area. Home Dish Satellite reached 1.2 million cable customers and 80,000 satellite-equipped homes.[37] Despite the fact that viewers had to purchase a $350 decoder and pay $150 subscription fee, both federal and some state laws were violated by these broadcasts. According to the then Attorney General, Dick Thornburgh, "The proliferation of cable and satellite dish technology has made it necessary for the Congress and the Department of Justice to act to prevent the pollution of the public airwaves with hard-core pornography."[38] Content issues such as pornography raise a number of issues, particularly in the U.S. where there are local, federal and constitutional issues that can be involved. In the terrestrial cyberspace domain there have already been a number of issues in the area of libel, theft of intellectual property and harassment. One writer has argued:

> As society goes electronic, contacts that used to occur in the town square are being made over the phone lines. The problem is that there's no simple standard for deciding who should decide. Often phone companies end up calling the shots by agreeing or not agreeing to bill and collect for services offered by outsiders over their networks.[39]

While the laws may be clearer when it comes to rules of the road for printed material, the rules of the road are not yet developed in cyberspace.

When Turkey began preparing to broadcast satellite programming into the Turkish speaking Muslim ex-Soviet states they encountered some of the following concerns:

> One of the first hurdles in setting up the satellite system was securing broadcast agreements from government officials in the six Muslim republics, many of whom are Communist holdovers. To make these arrangements, the Turks moved quietly.
>
> "We did not want the Iranians to know what we are doing. They also are trying to get satellite TV," said Muzaffer Beca, a producer for television news here [in Turkey]. "If this would have been widely known, then I think the Iranians would have offered large bribes to ministers in the republics to keep us out. They know that Turkish and Western television programs will hurt their religion."[40]

Malaysia recently banned effeminate men from appearing on television because it fears such "weaklings" could damage the country's industrialization efforts.[41] In fact Malaysia has banned the use of private satellite dishes to receive direct international TV broadcast. According to Information Minister, Mohammed Rahmat, "We have rather strict censorship in this country--we want to know what is arriving from the sky."[42] In the spirit of media control, earlier this year the Indian government, "pulled the plug on MTV when the 24-hour music video channel played one too many sexy videos."[43]

V. A Synthesis

Using the INMARSAT example of unauthorized users we can see what legal implications are involved at each level of the model I have presented.

A. Origination:

This is when unauthorized access is obtained by hacking an INMARSAT analog terminal. It is a form of fraud which is generally accomplished by using a legitimate user identification number. The result is that a legitimate company may end up with a bill for calls that they never made. The legitimate user may then inform the INMARSAT signatory that they are unwilling to pay for these unauthorized phone calls leaving the signatory with the bill.

B: Transportation:

INMARSAT will send the signatory a bill for unauthorized use of space segment (actual use of the satellite capacity). Under contract the signatory would be responsible for paying INMARSAT.

C. Termination:

When unauthorized phone calls are terminated over the Public Switched Telephone Network (PSTN) the terminating carrier will bill the signatory or the operator of the land earth station.

D. Content:

If there is a high probability of unauthorized usage it is conceivable that the content of calls could be monitored to determine the origin of such calls.

Currently INMARSAT and its signatories are discussing a burden sharing scheme in order to share the costs of unauthorized usage. The signatories have argued that INMARSAT should share some of the economic pain because of the inherently design weaknesses in the analog terminals.

It is worth noting that the economic impact of unauthorized usage through the modification of terminals is substantially smaller than the old style problem of users simply not paying their bills.

Recently, a syndicate of computer hackers in Britain, Germany and Australia broke into the computer and telephone systems of three large

multinational companies in Singapore. They were able to use the company's satellite links to transmit data around the world.[44] Again, to determine what type of crimes occurred and where they took place it is helpful to look at the origination, transport and termination continuum.

VI. Conclusion

The ambitious meta-framework that I have provided above is not bullet proof. It is simply intended as a guide to assist us in better understanding where and when the realms of outer space and cyberspace collide and what issues are likely to be involved.

I have decided to provide the following quote to show the importance to the international community of cyberspace and satellites and also the future open endedness of the implications:

> Pulling a country's telecommunications plug, or at least plugging its international telecommunications links, has so far remained free of political powerplay, except for less effective bilateral actions like those of the US against Cuba or Vietnam.
>
> Sooner or later someone on the UN Security Council is bound to start mapping out the prospects of digital excommunication as an alternative to sending in troops. With broad international support it could be achieved immediately, be far more water tight than straight trade sanctions, and require little in the way of risk to military personnel. Is the telecomms community ready?[45]

Earlier in this paper India's concern regarding Pakistan's broadcasting of programming into its country was cited. British secret agents once coined the term the "Great Game" to refer to the contest for the hearts and minds in the political influence marketplace.[46]

Because of the enormous political power of satellite broadcast, the foreign affairs implications are extraordinary powerful. Often dictatorships and totalitarian governments do not want the people they govern to be able to receive broadcasts that originate outside of their country. Other governments may find it in their best interest to have the attention of the world's media in order to "spin" a story in some intended fashion.

Very importantly, the frontiers of cyberspace and outer space force us to reconsider some of our basic preconceptions. Not only do we have to think in a multidimensional fashion, to be everywhere and nowhere simultaneously, these frontiers force us to rethink what it is to be human.

This paper is intended as a beginning point and not an ending point. The framework that I have offered provides analytical utility. However, there are many satellite crime issues that are difficult to easily categorize and can arguably be placed in several of the categories in the framework outlined above. Currently space law in this area is primarily confined to ITU regulations and treaties of the international satellite organizations. Origination and

termination issues primarily fall under the jurisdiction of specific national laws. As cyberspace and outer space become increasingly internationalized, there will probably be a need for international treaty law in the area of satellite crimes. Some are already calling for a stronger ITU or World Trade Organization with enforcement powers. This intersection of outer space and cyberspace will continue to generate more complex issues, despite any issues that may be resolved. The first challenge for those of us who struggle with these issues is first identifying where these issues are centered. Second, and perhaps the greatest challenge will be for those who have to legislate and enforce laws that involve the instantaneous transcendence of national boarders and jurisdictions.

Notes

[1] Michael Benedikt Ed, "Cyberspace: First Steps," Cambridge, MA, The MIT Press, 1991, pg. 14-16.

[2] Kaplan Sommer, Allison, "Hooked on Internet," The Jerusalem Post, May 6, 1994, pg. 12.

[3] When warned to consider the power of the Pope, Stalin is reported to have asked "how many divisions does the Pope have?"

[4] CompuServe Encyclopedia.

[5] Michael Benedikt Ed, "Cyberspace: First Steps," Cambridge, MA, The MIT Press, 1991, p. 1.

[6] Michael Benedikt Ed, "Cyberspace: First Steps," Cambridge, MA, The MIT Press, 1991, p. 8.

[7] "Religion and Communications: Feeding Fundamentalism," The Economist, August 21, 1993, pg. 34.

[8] Michael Benedikt Ed, "Cyberspace: First Steps," Cambridge, MA, The MIT Press, 1991, pg. 20-21.

[9] "Sardinian Challenges Polish T.V. laws," Financial Times, August 13, 1994.

[10] "GTE Spacenet Named in Porn Case," Space News.

[11] "Obscenity Charged Against Satellite Adult-Movie Channel and Others," Communications Daily, February 21, 1990, pg. 2. Also see "Cable Television Leased Access," The Annenberg Washington Program in Communications Policy, 1991, for an interesting discussion on the notion of cable providers as having a duty as common carrier and not as censor for content. See also Geller, Henry, "Fiber Optics: An Opportunity for A New Policy," The Annenberg Washington Program for in interesting discussion of the first amendment and broadcasting.

[12] The distribution of obscene matter by means of subscription services on television, by cable or satellite is a violation of Title 18, United States Code, Section 1468 (a).

[13] "Canadian Firm Beams Hard-Core Porn into US Homes," The Reuters EC Business Report, February 1, 1994.

[14] Treaties in Force 209 (U.S. Department of State, October 31, 1956). The Treaty was signed in Paris May 4, 1910. Protocol to the Treaty May 4, 1949.

[15] Coll, Steve, "MTV Age Dawning in India: Satellites Bring In Uninvited Guests," The Washington Post, March 5, 1992, pg. A38.

[16] Fisher, David, Prior Consent to International Satellite Broadcasting, Martinus Nijhoff Publishers, The Netherlands, 1990.

[17] Coll, Steve, "MTV Age Dawning in India: Satellites Bring In Uninvited Guests," The Washington Post, March 5, 1992, pg. A38.

[18] Will, George, "Suing the Swedish Bikini Team," The Washington Post, December 1, 1991, pg. C7.

[19] Telephone interview with Mr. David Sagar of INMARSAT 8/19/94.

[20] "Virginia Man Sentenced For Satellite Interference," SpaceNews, December 17-23, 1990.

[21] Informal discussion with employees at Belcom and PanAm Sat.

[22] Hollye, David, "Tokyo Says New Chinese Satellite Violates World Pact; Telecom: Apstar-1 was Squeezed into an Orbit Between Russia's

Rimsat and Japan's Sakura 3A," The Los Angeles Times, July 25, 1994, Part D, Page 5.
[23] Page, Shelley and Hum, Peter, "What Happened to Anik?; Theories abound, but Some Experts Suspect Design Defect," The Ottawa Citizen, January 29, 1994, pg. A1.
[24] "Charges After Decoding Probe," Financial Times, September 9, 1994
[25] "Problems of Videocrypt Piracy Out in Open," Screen Digest, November 1993.
[26] San Diego Union-Tribune, January 31, 1993.
[27] "Draft General Report of the working Group on Telecommunications and Media on Problems Relating to the Secrecy of Telecommunications and Satellite Communications and Draft Resolution o the XIV International Conference o data Protection and Privacy Commissioners in Sydney (27-29 October 1992) approved by the Working Group at its 12th Meeting (Berlin 28-29 September 1992) pg. 1.
[28] Wilson, John, "Configuring to Receive INMARSAT," Monitoring Times, March 1994, pg. 16-18.
[29] Sullivan, Jack, "Monitoring Space Shuttle Communications," Monitoring Times, March 1994, pg. 8-12.
[30] Messmer, Ellen, "Wiretap Legislation to Put Telecom Carriers Under Close Surveillance," Network World, August 15, 1994, pg. 6.
[31] "Va. Man Fined for Jordan Deal," The Washington Post, December 15, 1991.
[32] Stern, Chester, "Hackers' threat to Gulf War Triumph; Trio Played Havoc with Weather Computer Before Iraq Attack," Mail on Sunday, March 21, 1993 pg. 15. Actually the Cray is capable of making considerably more calculations per second.
[33] Smith, Elliot Blair, "Soviet Defense Technology Under Siege; Western Computer Hackers Track Outdate Satellites," The Houston Chronicle, August 1, 1994, pg. 8.
[34] "The Chairman," Reuters, 156 words, February 25, 1994.
[35] "International Shared Revenue Services: Reaching The Part that Domestic Services Can't Reach," Voice+, July/ August 1994, pg. 30.
[36] "International Shared Revenue Services: Reaching The Part that Domestic Services Can't Reach," Voice+, July/ August 1994, pg. 30.
[37] "'A National Scandal' Home Dish Satellite Networks Driven Out of Business on Obscenity Charges," Satellite Week, May 7, 1990, pg. 5-6.
[38] "X-Rated Satellite Broadcaster Pleads Guilty," Press Release, U.S. Department of Justice, November 29, 1990, p.1.
[39] Coy, Peter and Galen, Michele, "Lets Not Let Phone Pollution Hang Up Free Speech," Business Week, August 19, 1991, pg. 32.
[40] Harden, Blain, "Turkey Pushing Eastward--by Satellite: Muslim Ex-Soviet States Are Focus of Cultural, Commercial Plan," The Washington Post, March 22, 1992, A 31.
[41] "Malaysia Bans 'weak' Men From TV," International Herald Tribune, August 19, 1994, pg. 2.
[42] "Malaysia Clamps Down on Private Satellite Dishes," Space Fax Daily, August 2, 1991.
[43] "India lawmakers seek Curb on Sex," UPI, August 10, 1994.
[44] Mehta, Harish, "Three MNCs in S'pore lose millions to hackers," Business Times, October 7, 1992, pg. 1.
[45] "Feel the Political Clout of the Networks," Communications International, Volume 21, Number 7, July 1994, pg. 2.
[46] Harden, Blain, "Turkey Pushing Eastward--by Satellite: Muslim Ex-Soviet States Are Focus of Cultural, Commercial Plan," The Washington Post, March 22, 1992, A1.