COMMUNICATIONS
FORUM

SATELLITE JAMMING

Edward Horowitz, Home Box Office
Renville McMann, CBS
Ron Katznelson, M/A-COM, Inc.

October 16th, 1986

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

MASSACHUSETTS INSTITUTE OF TECHNOLOGY
COMMUNICATIONS FORUM

SATELLITE JAMMING

Edward Horowitz, Home Box Offfice
Renville McMann, CBS
Ron Katznelson, M/A-COM, Inc.

October 16th, 1986

Genga Arulampalam, Rapporteur

SATELLITE JAMMING

Edward Horowitz - Home Box Office

Horowitz began by briefly defining satellite jamming and alluded to the threat this could cause to society if resorted to by terrorists or even pranksters. He then identified the different phases in satellite transmission and methods by which jamming could occur. These are as follows:

- Uplink (as in the Captain Midnight situation)
- Downlink
- Transponder (such as to override or interfere with an on-going program)
- Move the satellite
- Blow-out the 'satellite tuoe'

Broadly classifying, satellite jamming could be divided into two types; accidental, and intentional jamming. Most jamming he said is accidental in nature and takes place in the uplink portion of transmission. Usually it is caused by inexperienced operators who while orienting their 'dish' sweep the skies from one satellite to the other jamming everything. This type of interference could be tracked down but usually is very temporary.

Horowitz then related the Captain Midnight incident that occured on April 27th 1986. While HBO was operating as normal, using a power of 125 watts through a 11 mm antenna (which is adequate to saturate the transponder), the intruder came in at about 250 watts in an attempt to "wrestle" the transponder away from HBO. The technicians on duty operating on standing instructions jacked-up the broadcast power (in an attempt to maintain control) upto 200 watts. But the intruder kept increasing the power of his transmission accordingly. Therefore,

fearing an over saturation (and subsequent damage) of the transponder, HBO pulled off the air. Captain Midnight thereby had the transponder to himself for 4 minutes. The interrupting message was basically a warning that dish dealers and owners were not pleased with HBO's scrambling of services since January this year. However, Horowitz stated that this displeasure was only among a small portion of dish owners and that primarily because of misrepresentations on the part of dealers. Aside from this small group of displeased dish owners the general response to dish sales and programs have been fairly dramatic - starting with 500 orders per week it is now over 3000 orders per week, with growth continuing in the right direction.

Referring to discussions a few weeks prior to this incident with both the White House and the FCC, Horowitz said that the general response from the government at that time to the possibility of this kind of threat was negative. He asserted that jammers are effectively communication terrorists who undermine the societal balance. Jamming he said could happen to anyone anywhere. However, the brighter side of the Captain Midnight incident is that the FBI and FCC responded immediately in efforts to track down Captain Midnight and also subsequently fought for preventive measures. A study of the recording enabled them to identify the type of signal generator that was used. Assessing the equipment at various uplink sites and the power that was used helped narrow down the possible sites from 2000 to about 200 to 300 and thereby track down the intruder.

Horowitz stated that what was of greater concern

however was what could happen from a backyard or mobile signal generator. For less than $5000 a person can put together a system capable of interfering with the satellite signal and even degrade the transponder. Since this kind of system could be built without any record or license, a suggestion made by HBO to the FCC relates to developing an identifying system.

In summary, Horowitz said that if the situation were to occur today there are procedures that would allow them to pin-point within a radius of a few 100 miles about 5 minutes after the transmission as to where it was coming from. This is done by allerting a few predesignated satellite carriers and by doing something at the uplink stage. While they cannot stop it happening they can find the person quite quickly. In the longer term he said a new generation of satellites are being developed that would have adequate protection.

The government he said realizes the vulnerability of its traffic and has (a) ordered 50,000 scrambler 'phones - a moderate level security (not encrypted), (b) installed a fiber optic network. The military he said, in his opinion, uses frequency-hopping for security purposes. Satellites he said, from the commercial perspective, will continue to remain vulnerable though less than before. He was also of the opinion that in the future satellites would not be used as much as at present.

Ron Katznelson - M/A-COM, Inc.

Katznelson addressed the issue of satellite jamming

beginning with the history of encryption relating to satellite-television communication. He stated that M/A-COM initially became involved by developing 'Videocipher'.

Videocipher I was developed allowing the encryption of the audio, first by digitizing it and then using DES to encrypt the bit stream which is placed in the horizontal blanking interval of the video signal, thus eliminating the need for audio subcarriers. The video is hard-scrambled by line dicing and permutation. The system was first tested by HBO around 1983. However, both HBO and M/A-COM recognized the need for a much lower cost system to be used as consumer decoders. Since it was not felt that the consumer business of digital video processing could economically sustain the cost even though it offered transmission security, Videocipher II with soft video scrambling was developed. HBO he said, pioneered the use Videocipher II and protecting transmission by scrambling in 1985. Actual continuous scrambling began on January 15th, 1986.

As a result of scrambling and also due to the confusion a reduction in the TVRO equipment market was anticipated. The uncertainities caused the reduction in sales of satellite receivers and dishes, causing an estimated loss of sales in the order of $400-$500 million per annum. This also brought with it the threat of satellite jamming.

Katznelson stated that there is some belief in the industry that the main motivation for "piracy acts" (satellite jamming) result from a perception of financial loss rather than an individual's inability to receive programming.

Katznelson stated that prior to the Captain Midnight incident other interference events had occured (e.g. Eastern Microwave) causing them to complain to the FCC. While it was not clear to the FCC or anyone else at that time as to whether the Eastern Microwave incident was accidental or not, the concern stimulated the FCC to begin investigations. The Captain Midnight episode that followed, expedited the FCC's notice of proposed rulemaking on an automatic identification of all uplink communication on the respective signal. Though this would not preclude intentional jammers it would eleminate/reduce accidental jamming and help identification. Currently, the identification is done by the SID (Station Identification Device) which is used in the vertical blanking interval. The FCC now requires that the identification signal be free of scrambling or encryption so as to be easily monitored and identified. Without a decryptor therefore, the actual signal that is being encrypted or secured has to be sent in an unrelated way. The other FCC requirement is that there should be no degradation in the signal. This prevents the insertion of a video subcarrier in addition to the signal. Katznelson stated that this is the kind of system they are currently working on.

Katznelson said that the main problem this would solve is one of identification, because a knowledgeable technician could still get into the hardware and disrupt/disconnect the identification cycle if he wishes to disable the SID. This calls for a new generation of transmitters in which the identifiers are an integral part. However he asserted that the SID or the ATIS (Automatic Transmission Identification System) is not a complete

solution but would help a little.

In closing, Katznelson stated that encryption/ scrambling does not make any difference to the vulnerability of a signal to jamming. He further added that it would be nice to look at other technologies which could help to limit/diminish the threat of satellite jamming. One area that yields scope for research is the spread spectrum. He also mentioned that the threat of jamming could eventually push towards larger research spending to find a suitable solution even though the current economies do not justify it.

Renville McMann - CBS

McMann began by briefly discussing the Automatic Identification Signal (AIS). CBS he said, together with its affiliates uses about 200 satellite news gathering trucks that are out in the field. These together with trucks used by other networks total as many as 600 mobile uplinks all using the K-band and capable of interfering with each other and with on-going program transmissions. In order to reduce interference, CBS encourages its news people, who use the uplink, to first go into a receiving mode and locate the satellite they want to transmit to, then turn on the transmitter at very low power looking with a spectrum analyser for the appearance of a low power carrier. If everything is alright they go into full power transmission.

He said that unlike HBO, which broadcasts via the

satellite direct to hundreds of thousands of receivers, CBS uses the satellite to transmit for example between New York and California to enable the program go out "live" on the network. This gives rise to the possibility of a jammer threatening to "black-out" millions of dollars worth of advertising by jamming 3 or 4 minutes of crucial programming. McMann said that while CBS has some operating procedures which they hope will help them overcome such a situation it still isn't a sure thing. He asserted that such an occurance today could cause trouble, while hopefully next year they would be in a position to overcome it.

McMann used slides with relevant specifications (exhibits A and B) to describe the functional relationship between the satellite and the ground receiver. The FCC he said limits the ground power to a maximum of 142 dbW/M2 in order to avoid jamming terrestrial microwave telecommunication going on in the same frequency. Taking into account the square of the distances between a jammer and the ground receiver, and the satellite and the ground receiver, a signal of the same power from a jammer 2.3 miles away would be more powerful by a factor of 100 million times (i.e. 80 db greater). Therefore a jammer of much smaller capacity (1 watt, 10 db antenna) could effectively perform this function from a distance of 2.3 miles from the ground receiver. Such a jammer he said, could easily be concealed and operated sufficiently close to the ground receiver to achieve the jamming effect. He cited the possibility of locating such a jammer on a radio controlled model airplane, thus not only successfully jamming the signal but also maintaining anonymity. CBS he said, in the short term, plans to use a back-

up antenna, and in the long term fiber optic cables to overcome this threat.

Another source of worry, according to McMann, is the possibility of "knocking-out" the uplink to a satellite using a magnetron (which could easily be found even in $200 microwave ovens) suitably adjusted for a 50 to 100 kilo watt pulse to occur during the sink or color burst interval, and in the case of scrambling, during the scrambling interval, to "knock out" the signal with the large peak power.

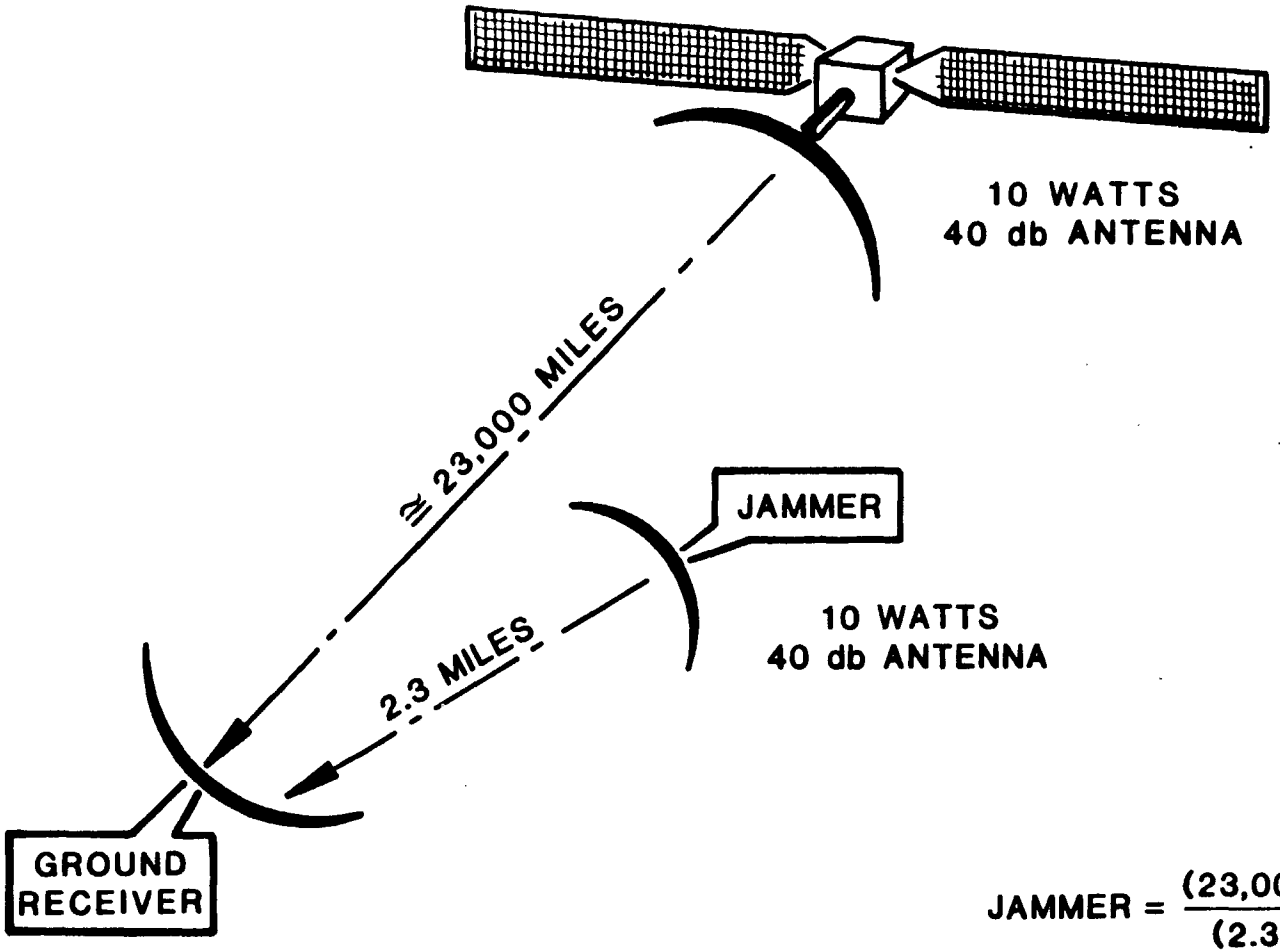
In closing McMann stated that most of these seemingly threatening situations have appropriate cures.

Speakers' Comments and Answers to Questions

A member of the audience inquired as to the extent of power used in the Captain Midnight incident and how much the satellite could withstand without being damaged. Horowitz stated that the intruder went upto 3000 watts which together with their 2000 watts totalled 5000. He further added that the satellite could withstand 4 times that power factor for upto 6 hours without sustaining damage.

A question was asked about broadcasting propaganda via satellite in Eastern and Western Europe. In response, Horowitz stated that broadcasting of almost anything was possible via unused satellite transponders. However, he asserted that this

type of propaganda broadcasting, particularly in Europe, was of limited value because of the limited market for satellite broadcast reception.



$$\text{JAMMER} = \frac{(23{,}000)^2}{(2.3)^2} = 100{,}000{,}000 \text{ TIMES}$$

AS POWERFUL AS WANTED SIGNAL,

i.e., 80 db GREATER

EXHIBIT : A

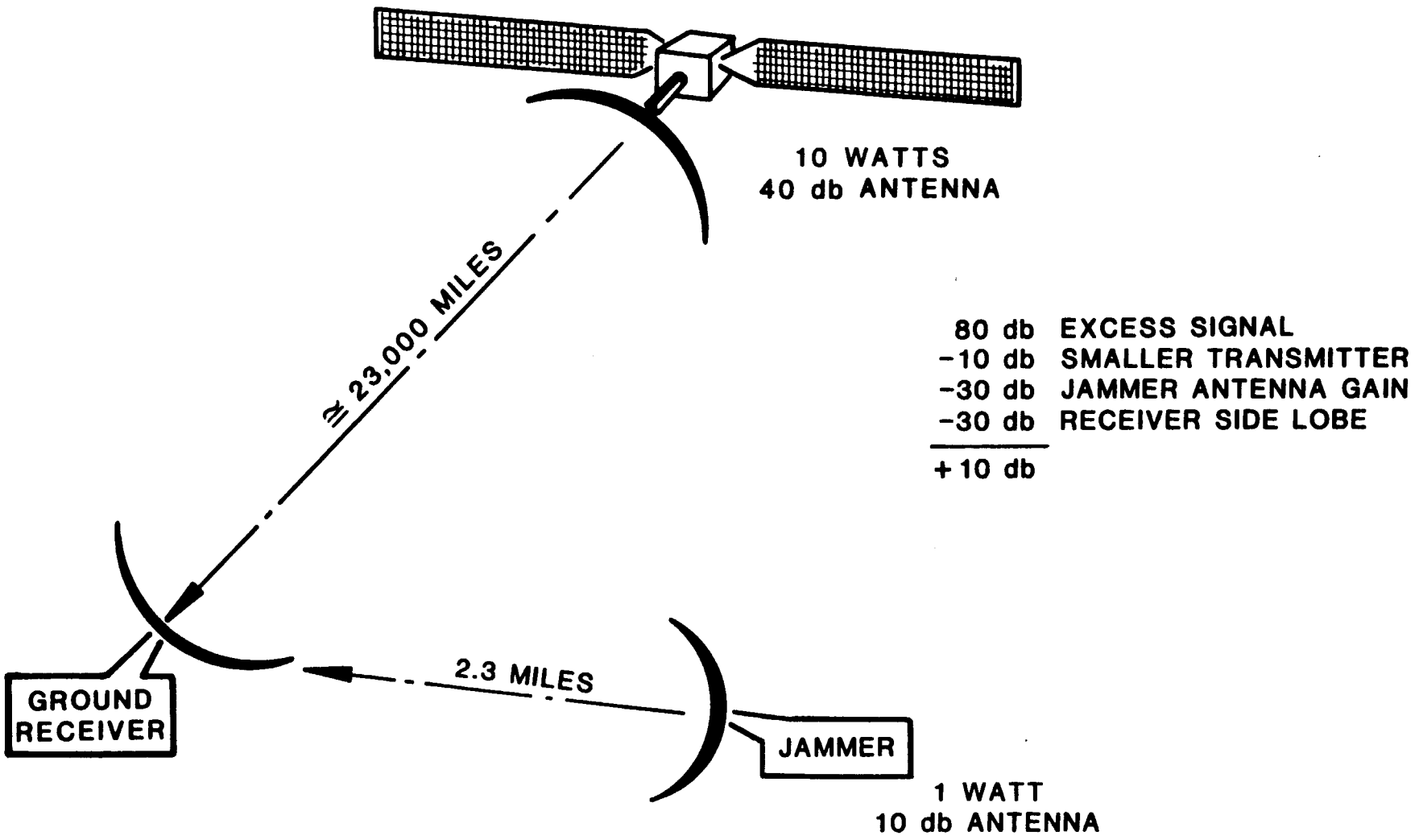

10 WATTS
40 db ANTENNA
≅ 23,000 MILES
80 db EXCESS SIGNAL
-10 db SMALLER TRANSMITTER
-30 db JAMMER ANTENNA GAIN
-30 db RECEIVER SIDE LOBE
+10 db
2.3 MILES
GROUND RECEIVER
JAMMER
1 WATT
10 db ANTENNA

EXHIBIT : B