

CHAPTER 3

THE ROLE OF NON-STATE ACTORS IN OUTER SPACE SECURITY

Jeffrey Lewis

NON-STATE ACTORS IN OUTER SPACE

The “terrorist” threat to space assets has largely been a minor concern in the dialogue about sustaining the common interest in the peaceful uses of outer space. An exception to this rule was the Congressionally-empanelled Commission to Assess US National Security Space Management and Organization (Space Commission), which warned that threats to US space systems “might arise under a variety of conditions” including during “peacetime, as a terrorist act”.¹

The topic raises a number of interesting questions—questions that are easier to raise than answer. For example,

- It is always difficult to define terrorism. Is an act of terrorism one that kills people? What about an act that only destroys property? Must an act of terrorism kill a person or destroy property, or is it merely enough to generate fear or chaos? Terrorism also carries a certain normative connotation, that is, one’s enemies may be terrorists, but one’s friends may be freedom fighters or liberationists.
- What is special about “space” terrorism, as distinct from more mundane, if that is the right word, forms of terrorism? Is a terrorist who hacks into a computer network to attack the financial system doing something manifestly different if the network manages satellites instead of bank transfers? What if a terrorist attacks a ground station or a spacecraft about to launch? Are those acts different from attacks on embassies or aircraft?

Yet, the relationship between terrorism and outer space is part of a larger, overlooked dialogue about the increasing role of non-state actors in outer space.

Since the dawn of the space age, the exploration and peaceful uses of outer space have been the province of governments. The primacy of states as actors in space is captured by the Convention on International Liability for Damage Caused by Space Objects, which assigns the responsibility for damage caused by an object in space to the state that launched the object.

That decision reflected the reality of the 1960s. Today non-state actors play an increasing role in the uses of outer space. Universities build small, capable satellites. Dissident groups broadcast their complaints on commercial communications satellites. A small number of very wealthy individuals have purchased “vacations” on the International Space Station. More may soon have the opportunity to enjoy a suborbital flight and experience a few seconds of weightlessness. Only launch services appear to remain a fundamentally national endeavour, although here too some firms are looking toward the future in the private sector.

The growing presence of non-state actors in outer space, combined with our growing dependence on space assets, raises a series of interesting questions about the security of our space assets—a point the Space Commission makes rather plainly:

The relative dependence of the U.S. on space makes its space systems potentially attractive targets. Many foreign nations and non-state entities are pursuing space-related activities. Those hostile to the U.S. possess, or can acquire on the global market, the means to deny, disrupt or destroy U.S. space systems by attacking satellites in space, communications links to and from the ground or ground stations that command the satellites and process their data.²

I focus on the implication of *all* non-state actors for sustainable uses of outer space; that is to say, a number of real examples involving non-state actors that are not necessarily terrorists by addressing two questions:

- What challenges do non-state actors pose for the peaceful uses of outer space? and

-
- How should governments and international institutions respond to the increasing presence of non-state actors in outer space?

In general, I do not think non-state actors pose much of a threat to space assets, largely because even states have not developed advanced anti-satellite technologies. This conclusion is based, in part, on unclassified intelligence estimates and official US statements. That said, I believe non-state actors pose a number of challenges to the peaceful uses of outer space that might usefully be part of a larger dialogue on the effect that greater access to space has on building a sustainable space security architecture.

CHALLENGES POSED BY NON-STATE ACTORS

PHYSICAL ATTACK AGAINST THE INTERNATIONAL SPACE STATION, SPACE SHUTTLE OR PRIVATE SPACECRAFT

Perhaps the only traditional “terrorist” scenario is that a group of individuals somehow hijack the Space Shuttle or International Space Station. This is the subject of countless science fiction novels and at least one mean-spirited conspiracy theory.

In the wake of the terrorist attacks of 11 September 2001, the National Aeronautics and Space Administration (NASA) did impose additional security surrounding the launch of STS-108 in December 2001.³ A NASA administrator at the time, Sean O’Keefe, told reporters:

There is no question (the Space Shuttle) is a high-value target. It has been identified as such by all the intelligence information that we had received post-Sept. 11, that this is considered to be a very high-value target opportunity that terrorists view as a great way to make a statement.⁴

Overall, however, the risk of such a scenario, according to a group of non-governmental experts from The George Washington University, “seems remote to most people involved in the US space programme since the Space Shuttle facilities are reasonably well protected and that once in space the vehicles are physically remote from any would-be attackers”.⁵ A more likely threat is that terrorists might attack the ground stations that are

used to control space assets, either physically or through some form of hacking.

An interesting case arises with regard to private firms offering suborbital flights as “space tourist” expeditions: perhaps some passenger might attempt to seize control of one of these craft. The US Federal Aviation Authority, which would regulate space tourist flights, has proposed security restrictions similar to those imposed on passengers on commercial airlines, including a recommendation that the operator consult the Transportation Security Agency’s “no fly list”.⁶

JAMMING SATELLITE COMMUNICATIONS OR ATTACKING GROUND STATIONS

“Jamming” is the transmission of signals that interfere with the operation of a satellite or its payload.⁷ Generally, it has been states that have jammed broadcasts by non-state groups and other states. As recent examples, the Rumsfeld Space Commission cited “Indonesia jamming a transponder on a Chinese-owned satellite and Iran and Turkey jamming satellite TV broadcasts of dissidents”.⁸

In the case of the dispute between China and Indonesia, APT Satellite of China reported “limited interference” with its Apstar-1A satellite from another satellite in a nearby orbital slot that was operating on the same frequency. Although the commission calls the interference “jamming”, the interference resulted from satellites operating too close together because the countries disputed the ownership of the orbital slot. The dispute was eventually resolved peacefully.⁹

The Islamic Republic of Iran and Turkey are reported to have jammed satellite broadcasts by dissident groups. A Kurdish television station claimed that the Turkish government jammed its broadcasts; the Islamic Republic of Iran, operating from the Iranian Embassy in Havana, jammed a dissident radio station.¹⁰ In the case of the Islamic Republic of Iran, the United States reportedly pressured Havana to stop the jamming originating from the Iranian Embassy.¹¹

Two cases of non-state entities briefly interrupting satellite transmissions bear mention. In 1986, an American using the name “Captain Midnight” briefly interrupted a cable programme to protest the cable

channel's fee structure. John R. MacDougall, a 25-year-old satellite dish dealer and electronics engineer, later pleaded guilty to violating a Federal Communications Commission (FCC) statute against "broadcasting without a license".¹² More recently, in 2002, the Chinese government accused a Taiwan-based Falun Gong group of interfering with Chinese satellite television signals. Taiwanese authorities claim to have investigated and found no evidence of these activities.¹³

A special case of jamming might involve a non-state actor who could attempt to use a commercially available global positioning system (GPS) jammer to interfere with a plane while it is attempting to land. Commercial aircraft do not, however, rely exclusively on GPS signals for navigation. US Air Force Lt. Col. Ken McClellan, a Pentagon spokesman, told *Computer World* that although jammers "could disrupt commercial operations", the Pentagon viewed homemade jammers as "a nuisance" rather than a hazard to commercial aircraft and ships.¹⁴

OTHER CHALLENGES POSED BY NON-STATE ACTORS

There are two other ways in which non-state actors raise interesting questions about the uses and misuses of access to outer space.

One challenge is posed by non-state actors using commercial satellites for communications or imaging. Following the 11 September 2001 terrorist attacks against the United States, some observers worried that terrorists might use commercially available satellite images to aid in planning attacks, although terrorists arguable require more timely and detailed information than is available from commercial imagery.¹⁵ Commercial availability of images and communications is widely accepted as a beneficial development; nevertheless, a sensible dialogue about the peaceful uses of outer space should reflect the potential for misuse of such services. In the months before Operation Enduring Freedom in Afghanistan, the United States purchased exclusive access to commercial images taken by Space Imaging's Ikonos satellite, at least in part to deny those images to the Taliban.

A second challenge emerges from the greater access to space experienced by non-state actors, including private launch services and the development of very small, but capable, satellites. The world's leading builder of "micro-satellites" is the university-based firm Surrey Satellite

Technology Ltd (SSTL), which is developing a constellation of remote sensing micro-satellites for natural disaster monitoring and mitigation.¹⁶ Some American observers have expressed concern about SSTL's role in helping Chinese scientists at Tsinghua University build and launch TsinghuaSat-1, a micro-satellite containing a multispectral camera with 40-metre resolution. One area worth considering is the development of satellites that are capable of on-orbit manoeuvres around other satellites, so called autonomous proximity operations. During the launch of TsinghuaSat-1, SSTL also launched SNAP-1, built by SSTL alone, which was designed to conduct proximity operations near TsinghuaSat-1. SNAP-1 successfully manoeuvred to within 9 metres of the Chinese satellite, transmitting a digital image.¹⁷

CONCLUSION

The ongoing dialogue among all countries that rely on the peaceful uses of outer space remains important. This dialogue should be expanded in a number of areas to include interference, traffic control, mitigating debris and future proximity operations. Including actors such as Intelsat will be necessary in order to create practices that meet the needs of all space users.

States should not, however, disrupt existing efforts to protect space assets on behalf of terrorism. Physical threats to space systems can, and should, be dealt with at the national level. States might share best practices to discourage jamming from originating within their territories. In the United States, all satellite uplink transmissions carrying broadband video information contain an "automatic transmitter identification system" that provides the station's FCC-assigned Earth station call sign, a telephone number and serial number. This practice, adopted after the Captain Midnight episode, largely prevents individuals from jamming satellites anonymously.

Notes

- ¹ United States Department of Defense, 2001, *Final Report of the Commission to Assess US National Security Space Management and*

Organization, January, Washington, DC. (Hereafter, the *Final Report of the Space Commission*.)

- 2 *Final Report of the Space Commission*.
- 3 Mark Carreau, 2001, NASA on Mission for More Security: Tighter Rules Will Mark Shuttle Liftoff, *The Houston Chronicle*, 26 November, p. A6.
- 4 Mark Carreau, 2002, Space Security Beefed Up: NASA Tightens Public Access in 9/11 Aftermath, *The Houston Chronicle*, 7 September, p. A14.
- 5 Space and Advanced Communications Research Institute, 2005, *Space Safety Report: Vulnerabilities and Risk Reduction In U.S. Human Space Flight Programs*, April, Section 4.4, Washington, DC, George Washington University.
- 6 United States Federal Aviation Administration, *Human Space Flight Requirements for Crew and Space Flight Participants, Notice of Proposed Rulemaking*, FAA-2005-23449, 22 December 2005, p. 38, at <dms.dot.gov/search/document.cfm?documentid=378657&docketid=23449>.
- 7 United States Army Space Institute, 1993, *Threats and Countermeasures: Other Threats From Deliberate Attack*, Army Space Reference Text, July, Chapter 8, Section 4, Fort Leavenworth, KS.
- 8 United States Department of Defense, *Rumsfeld Space Commission Report*, p. 20, Washington, DC.
- 9 For a review of the APSTAR incident and other disputes over orbital slots, see ITU System of Satellite Coordination Eroding Fast in Asia Pacific, *Space Business News*, 2 April 1997; Richard McCaffrey, Crowded Orbital Slots Test ITU's Influence: Dispute at 134 Degrees East Highlights Problems, *Space News*, 7 January 1997.
- 10 Nora Boustany, Kurdish TV Gets Static from Turks, *The Washington Post*, 25 November 1998, p. A16; U.S. Waits for Formal Cuban Response on Jamming of Satellite Broadcasts to Iran, *Voice of America News*, 22 July 2003.
- 11 Cuba Stops Iran From Jamming U.S. Broadcasts, *Voice of America News*, 20 August 2003.
- 12 Peter J. Boyer, HBO Piracy Incident Stuns Other Satellite Users, *The New York Times*, 29 April 1986, p. C17.
- 13 *China (includes Taiwan only)*, 2004, International Religious Freedom Report 2004, released by the Bureau of Democracy, Human Rights, and Labor, China, 15 September.

- ¹⁴ Bob Brewin, 2003, Homemade GPS Jammers Raise Concerns, *Computer World*, 17 January, at <computerworld.com/securitytopics/security/story/0,10801,77702,00.html>.
- ¹⁵ See, for example, John C. Baker, 2001, Commercial Imagery: Potential Perils?, *Imaging Notes*, November–December, at <www.imagingnotes.com/old/novdec01/global_trans.htm>.
- ¹⁶ You Zheng and M. Sweeting, *Initial Mission Status Analysis of 3-axis Sable Tsinghua-1 Microsatellite*, 14th Annual AIAA/Utah State University Conference on Small Satellites, Logan, UT, 21–24 August 2000; Xiong Jianping et al., *On board computer Subsystem Design for the Tsinghua Nanosatellite*, 20th AIAA International Communication Satellite Systems Conference, Montreal, 12–15 May 2002.
- ¹⁷ See the SSSL web site for SNAP at <zenit.sssl.co.uk/index.php?loc=47>.