



By Gerry Oberst

Protecting Satellites From Space Terrorism

Is the security threat to satellites from possible terrorist acts being taken sufficiently seriously? The European Space Policy Institute (ESPI) thinks not and issued an article in January, titled “The Need to Counter Space Terrorism – A European Perspective”, arguing for studies to introduce effective counter measures to protect satellites.

The article on the need to counter “space terrorism” seeks to offer a European perspective. While writing that Europe does not depend to the same extent as the United States on military applications of space, the author says the European Union (EU) faces increasing vulnerabilities due to space programs such as the Galileo position location system and the Global Monitoring for Environment and Security (GMES) program Europe is championing. Moreover, as commercial satellites increasingly are used for military communications, the risk of attacks on military targets flows over to the commercial side in general.

“Satellites or space-based assets provide quite a potential target,” says the ESPI. In its view, terrorists are “both motivated and capable of conducting a terrorist attack in space.” The article focuses more on terroristic acts impeding military use of space resources but notes that terrorists will search out targets that can achieve mass casualties or have a lasting psychological effect.

The ESPI catalogs the options that terrorists might consider, including “disruption, denial, degradation and deception” of space systems. It does not explain exactly how any of these acts might contribute to mass casualties. The only discussion of how casualties might arise is hypothesized as the blinding of military intelligence satellite facilities rather than commercial facilities.

The article notes examples of commercial disruptions as evidence of possible risks. Thus, it lists three examples of jamming and piracy events that occurred in the commercial satellite sector: the 2006 jamming of the Thuraya mobile satellites from Libyan locations; the two-year episode when the Tamil Tigers hijacked an Intelsat transponder to transmit their separatist message across the Indian subcontinent; and shorter episodes when the Falun Gong disrupted satellite broadcast signals in 2004, including taking over AsiaSat signals for four hours.

The article claims these are “only

some recent examples,” even though there are very few other such episodes publicly reported. Nevertheless, the risk remains, and with increasing reliance on satellite-based location and positioning services, the disruption to society could be immense if those services were jammed.

Another recent assessment of these issues was published in August by Canadian-based SpaceSecurity.org. It provides a few more examples of jamming and an in-depth analysis of the risks. One of its conclusions is that the most vulnerable components of space systems are the ground stations and communications links. These components are susceptible to attack from widely accessible weapons and technologies. The ESPI agrees with this and says policy makers must consider the system architecture as a whole, even though the ESPI article seems focused on means to protect the satellites themselves.

Thus, the ESPI identifies a need to create market incentives for the protection of commercial satellites and says Europe needs to “develop its own identify and strategy in this regard.” It calls for more attention to space security studies at a time when Europe is seeking to identify its overall space strategy.

The ESPI discusses a wide range of possible approaches. For instance, it argues that future counter-terrorism policy for space should avoid relying on dual-use technologies, traditionally defined as technologies that are useful for both commercial and military applications, because these might be turned into space weapons. It refers as an example to small maneuverable satellites designed for inspecting other satellites in space, which might also be used for military applications.

The ESPI proposes developing a common European export control regime for transfer of conventional arms and dual-use technologies as one means to limit technology from harming satellites falling into the wrong hands. The U.S. satellite industry has suffered for years under such a policy, which industry argues has substantially impeded commercial export of high-tech equipment. European industry should be careful in its recommendations in this respect.

The ESPI also seems to suggest reliance on operating satellites at the European level rather than by individual member states, so terrorists cannot target a particular country. This approach is unlikely to be welcomed by any satellite operator in Europe and raises an enormous number of institutional and political questions. ▮

Gerry Oberst is a partner in the Hogan & Hartson Brussels office.