Acta Astronautica 128 (2016) 409–415

Contents lists available at ScienceDirect

Acta Astronautica

journal homepage: www.elsevier.com/locate/aa

Cybersecurity threats to satellite communications: Towards a typology of state actor responses

Deborah Housen-Couriel

Interdisciplinary Cyber Research Center (ICRC), Tel Aviv University, Israel

ARTICLE INFO

Article history:
Received 24 February 2016
Accepted 8 July 2016
Available online 29 July 2016

ABSTRACT

Cybersecurity threats to satellite communications are a relatively new phenomenon, yet have quickly come to the forefront of concern for the sustainability of satellite systems due to the vulnerabilities that such threats may exploit and negatively impact. These vulnerabilities are mission-critical: they include launch systems, communications, telemetry, tracking and command, and mission completion. They and other aspects of satellite communications depend heavily on secure and resilient cyber capabilities for all stages of the satellite's lifespan. Because of the inherently global nature of both satellite and cyberspace activities, these capabilities rely significantly on international cooperation for setting a baseline of agreed legal norms that protect satellites and satellite communications. This critical cooperation is relevant during all mission phases, from planning to final wrap-up. Under optimal circumstances, the norms and standards protecting satellites and satellite transmissions are developed and enforced by those nation-state actors that are committed to system operability and overall mission sustainability for those satellites launched under their aegis and responsibility. However, when breaches of international law do occur in the form of hostile cyber events that cause damage to satellite communications, a range of measures should be available to the victim state, provided by the appropriate legal regime or regimes. This article proposes that a comprehensive and integrative multi-stakeholder review be undertaken in the near future of the measures available under international law for responding to hostile acts directed at satellite systems and communications, in a manner that takes into account both existing regimes of international law reviewed herein, as well as considerations of cybersecurity. These measures will depend upon the characterization of hostile interference with satellite transmissions in accordance with a proposed typology of hostile events. At present, four key normative international law regimes influence the types of measures that may be undertaken by states: the UN Charter's collective security regime; space law (governing the launching of objects and their space activities, including liability for damages); global telecommunications law (governing data transmissions and protection of infrastructures); and the substantive law relating to transborder freedom of information. Moreover, the nascent normative framework that will eventually apply to state and non-state activities in cyberspace will also be relevant to satellite communications, although it has been largely excluded from analyses and studies. In summary, this article proposes a typology of hostile events, both kinetic and cyber-enabled, that are liable to disrupt satellite communications; and it reviews the four key relevant legal regimes and notes the challenges of nascent cybersecurity law on the international plane. The article concludes by advocating for the establishment of a framework for effective elucidation of appropriate legal remedies at the international level in responding to kinetic, virtual and hybrid threats and hostile disruptions to satellite communications.

1. Introduction

Recent events around disruptions to satellite communications, such as the hostile activities carried out by the Turla hacking group by exploiting satellite-based Internet links [1]; and the distortion by other actors of GPS time signals [2], have brought this issue to the forefront of concerns among space-faring states [3]. Intentional disruptions of satellite communications raise challenging questions for international lawyers around the appropriate application of international law and the remedies it provides in response to such events. Moreover, the influence of nascent norms of cybersecurity law on the existing international law applicable to satellite communications suggests the need for a future re-framing of the legal debate in the broader context of the application of international law to the activities of nation-states, as well as non-

E-mail address: deborah@cyberregstrategies.com

http://dx.doi.org/10.1016/j.actaastro.2016.07.041
0094-5765/

state actors, in cyberspace. Until such point in time as legally-binding norms of state activities in cyberspace coalesce with some specificity, it is cautioned this necessary re-framing can only be tentative.

The new threats to international stability posed by the increased use of outer space by the more than 1000 registered and operational satellites currently in orbit [4], include both kinetic and virtual (or cyber) hostile disruptions of satellite transmissions. Such acts come under the general rubric of anti-satellite capabilities, or ASAT. They may incur physical harm to ground stations and satellites (by collision with another satellite or space debris, for instance); or harm causing disruption by interference with the digital communications systems of the satellite by virtual means such as jamming, distortion or other disruption of computerized guidance and communications systems [5]. A third category of hybrid ASAT disruptions, such as "satellite blinding" by laser, or an electromagnetic pulse (EMP), includes hostile events that combine kinetic and virtual elements of disruption in a hybrid manner of incurring damage to the targeted satellite.

Such hostile disruption of satellite communications is rapidly becoming a part of the strategic and tactical planning against ASAT of state, and some non-state, actors [6]. Physical threats to satellite systems have been brought to the fore by the announcement of several states new to the "satellite club" of satellite launches and other long-range ballistic trials, such as North Korea's satellite launch in February 2016 (which was condemned by the UN Security Council in violation of sanctions on that country) [7] and its ongoing ballistic missile trials, and Iran's February 2015 launch of the Fajr satellite [8]. Also, events such as the May 2013 Chinese launching of an upper-ionosphere research satellite [9], the January 2007 destruction by China of one of its own satellites, a similar initiative on the part of the US in February 2008, and other, less-known ASAT events have sent clear messages to the international community regarding capabilities and possible intentions of the initiating countries. That is, if one of their own satellites can be physically destroyed, there's no longer any doubt that rival satellites are feasible targets. [10].

In addition, in a hyper-connected world now characterized by the ubiquity of cyberspace activities [11], cyber-enabled disruption of satellite signals can pose an ongoing strategic and fundamental threat to states when the satellite communications control critical national and global critical infrastructures such as military systems, banking and financial systems, air traffic control, electricity grids, traffic and transport systems, early-warning weather systems, and the like [12]. In the words of one 2014 observer, these strategic threats are growing:

> "As space systems increasingly perform and support critical operations, a variety of plausible near-term incidents in outer space could precipitate or exacerbate an international crisis. *The most grave space contingencies [….] are likely to result from either intentional interference with space systems or the inadvertent effects of irresponsible state behavior in outer space"*[13]. (italics added)

ASAT of various types, including hostile interference with satellite transmissions, has also been treated as a critical issue in the context of the increasing militarization of space, as addressed under the auspices of the United Nations' Office for Outer Space Affairs (UNOOSA) and Office for Disarmament Affairs (UNODA). For example, in the 2013 Report of the UN Group of Governmental Experts on Transparency and Confidence-Building Measures in Outer Space Activities (herein, "GGE") it was noted that the outer space environment is becoming "…increasingly congested, contested and competitive. In the context of international peace and security, there is growing concern that threats to vital space capabilities may increase during the next decade as a result of both natural and man-made hazards and the possible development of disruptive and destructive counterspace capabilities" [14].

Ongoing work under the auspices of UN bodies and other intergovernmental organizations regarding the developing parameters of outer space governance has in recent years sharpened the understanding that a new, unified approach is needed [15]. The underlying assumption of this article is that international law has a key role to play in articulating these "rules of the road" for the activities of state actors relating to satellites, including the imposition of realistic and effective sanctions for those states that do not uphold and implement the applicable legal norms. Yet the additional and relatively unexplored issue of the application of international law to state activities in cyberspace is a relevant legal consideration that also needs to be weighed in evaluating the range of possible state responses to hostile disruption of satellite communications. This consideration is largely absent from existing intergovernmental initiatives regarding outer space governance [16].

2. The range of hostile disruptions

2.1. Kinetic, virtual and hybrid disruptions

Disruption of satellites and satellite transmissions may occur in all phases of the satellite lifespan. From the pre-launching testing phases, through launch into orbit, during the satellite's active lifespan, and through its de-activation, hostile disruptions are liable to effect transmissions [17]. These are distinguished, for the purposes of the following legal analysis, from disruption that occur through error or negligence, i.e. without hostile intent. Examples of kinetic, virtual and hybrid disruptions include, in sequence: (a) direct impact of one satellite with another, with intent to disable the former; (b) the jamming or other disturbance of telemetry, tracking and command (TT&C) transmissions or other satellite communications with intent to block or distort them; (c) directing an electro-magnetic pulse (EMP) at a satellite with intent to damage it physically, albeit via utilization of the electromagnetic spectrum, which is an element of cyberspace infrastructure [18].

2.2. A proposed typology

The proposed typology of hostile disruptions is based on a matrix that juxtaposes the means of disruption (kinetic, virtual, or hybrid) with the point at which the disruption occurs over the satellite lifespan, as described above. An example drawn from the full matrix is shown in Table 1 below. The juxtaposition of these elements is relevant to the legal regime that will apply to the event and that will determine the scope of responses available to the injured state or states. Thus, the sample matrix in Table 1 indicates the general application of the legal regimes reviewed herein.

There are particular legal ramifications when a hostile

Table 1
Typology of hostile satellite disruptions with applicable international law regime (Key: U=UN Charter regime; S=Space Law; T=Telecommunications Law; F=Freedom of Communications).

	Pre-launch	At launch	TT&C (ongoing)	Transmissions (ongoing)	End-of-life
Kinetic	U	U,S	U,S, F	U,S,F	U,S
Virtual	U,T	U,S,T	U,S,T,F	U,S,T,F	U,S,T
Hybrid	U,T	U,S,T	U,S,T,F	U,S,T,F	U,S,T