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

disruption affects particular content that is transmitted by the satellite, such as in Iran's disruption of Eutelsat transmissions including BBC Persian, the VOA Persian service and Radio Free Europe's Radio Farda [19]. More specifically, when the content rather than the satellite transmission capability in a technical sense is the object of hostile disruption, an additional legal regime may be applicable in the context of freedom of information across national borders. Thus, if one country initiates a kinetic or virtual disruption to satellite broadcasts that contain images or messages which have been particularly targeted because of their content, issues regarding freedom of information are likely to arise, although its present scope does not provide absolute assurance of the right to transmit all content. This point is further explored below.

3. Applicable international law regimes

Four principal legal regimes are salient to the analysis of harmful disruption of satellite communications: the collective security regime developed on the basis of the UN Charter, space law, international telecommunications law, and some aspects of transborder freedom of information. These regimes have some overlap in their substance, application and enforcement, and may best be characterized as intersecting and complementary [20]. For example, the Turla group's hack of satellite signals referred to above may implicate international telecommunications law, space law and freedom of information, through its harmful interference with transmissions.

In addition to the four regimes reviewed herein, currently emerging norms relating to cybersecurity will impact on the way in which states address intentional disruption to satellite communications. In response to the growing impact of harmful activities in cyberspace, state and intergovernmental actors have undertaken a number of initiatives to clarify the normative parameters of cyber activities in general [21]. Specifically, satellite communications are affected by these developing parameters, as they take place almost exclusively in cyberspace. In a study of the intersection of space security and cyber security, Baylon notes:

> Satellites, ground stations and other space assets rely increasingly on the internet and other cyber networks for their functions, which renders them vulnerable to cyber attack. For example, hackers could use internet-enabled remote configuration features to take control of a space system, resulting in anamolous behavior or even catastrophic failure of a satellite [22.]

Thus, the incorporation of cybersecurity considerations will be an important element of the analysis of harmful interference to satellite transmissions in light of the four regimes reviewed below.

3.1. The UN Charter's collective security regime

Satellite communications combine the physical, kinetic elements of the launch of an object into space, together with the non-kinetic elements of digital communications to and from the satellite. Hostile disruption of satellite communications on the part of state actors, as distinguished from error, negligence and other non-hostile motivations, raises questions under international law around the applicability of the UN Charter regime of collective security to such acts in cyberspace, and specifically whether they may constitute a use of force under the Charter's Article 2(4) [23]. These questions are particularly challenging when the disruptions are virtual or hybrid, rather than exclusively physical [24].

Several recent initiatives aim to elucidate the application of international law in general, and the collective security regime of the Charter in particular, to activities that take place in cyberspace, such as satellite transmissions utilizing the electromagnetic spectrum [25]. Many definitions of "cyberspace" – there is at present no single determinative definition in international law – include the electromagnetic spectrum as an element thereof. For example, the 2013 Tallinn Manual on the International Law Applicable to Cyber Warfare ("Tallin Manual") defines cyberspace as "The environment formed by physical and non-physical components, characterized by the use of computers and *the electromagnetic spectrum,* to store, modify and exchange data using computer networks." (italics added) [26].

The Tallinn Manual and other initiatives likewise engage with the issue of whether state activities conducted by virtual means in cyber space, if sufficiently damaging, may be held by victim states to constitute a "threat or use of force" in the meaning of Article 2 (4) of the UN Charter [27]. The international law has yet to be definitively settled regarding the parameters of the applicability of this provision to acts committed in cyberspace; as well as the permitted parameters of self-defense in response, for example, to disruption of satellite transmissions that may in the event be determined to constitute an "armed attack" under the Charter's Article 51 [28]. One example would be the intentional disruption of satellite transmissions that provide air traffic control towers with data on airplane traffic and navigation, causing aircraft accidents and consequent loss of life.

The as-yet unresolved issues of whether a virtual attack on a satellite system may constitute a use of force or armed attack under the Charter is a compelling one for an increasing number of states [29]. More and more, state and non-state actors are interested in knowing under what circumstances intentionally harmful disruptions to satellite transmissions may constitute an act that justifies self-defense; and what the parameters of legitimate response to such an act may be [30]. These are especially cogent issues given the contemporary key role of satellite communications in essential governmental, financial, military and commercial systems. Critical infrastructure that is dependent upon satellite communications is especially at risk to ASAT in this context [31].

3.2. Space law

Space law developed in the wake of the genesis of space exploration in the 1950s. The five space treaties and customary law relate to the activities in outer space of a relatively small community of space-faring states. The entire regime is currently under a process of review and evaluation as the 50th anniversary of the 1967 Outer Space Treaty (OST) [32] approaches, under the aegis of the UN Committee on the Peaceful Uses of Outer Space (COPOUS) [33].

Under the OST's Article I, outer space is defined and established as a physical realm available to all states for peaceful use and exploitation, as part of humankind's common heritage. Moreover, the article states that "Outer space, including the moon and other celestial bodies, shall be free for exploration and use by all States without discrimination of any kind, on a basis of equality *and in accordance with international law*" (italics added). This provision encompasses the collective security regime set out in the UN Charter and discussed above [34]. The four additional space law treaties, as well as a number of UN General Assembly resolutions and declarations address the applicability of the international law to outer space, including space objects such as satellites [35].

States may not claim sovereignty over locations in space, nor over moons or planets [36], yet they retain sovereignty and control over satellites and other space objects that they either own or launch into space. The OST also establishes states' liability for any damage caused by such objects [37]. Article VII is the operative provision, and it provides as follows:

"Each State Party to the Treaty that launches or procures the launching of an object into outer space, including the moon and other celestial bodies, and each State Party from whose territory or facility an object *is launched, is internationally liable for damage to another State Party to the Treaty or to its natural or juridical persons by such object or its component parts on the Earth, in air or in outer space, including the moon and other celestial bodies*." (italics added)

Thus, space law imposes upon states the responsibility for actions carried out by satellites under their jurisdiction and control, and duly attributable to them under international law. These actions may include physical damage caused by the creation of space debris that inflicts physical harm to other satellites.

The full regime establishing responsibility and stipulating damages is set out in the Liability Convention, which elaborates on OST Article VII. The degree of liability incurred under particular circumstances is stipulated in the Liability Convention's Articles II through VI. For instance, Article II establishes absolute liability "for damage caused by [the launching state's] space object on the surface of the earth or to aircraft flight" [38]. This liability requires, for example, payment of compensation to the injured state when certain criteria have been met. In outer space, state liability must be established in accordance with the provisions of Liability Convention Articles II and IV. For these purposes, "damage" is defined as: "… [the] loss of life, personal injury or other impairment of health; or loss of or damage to property of States or of persons, natural or juridical, or property of international intergovernmental organizations" [39].

There remains an open question of the applicability of the Liability Convention to satellite transmissions that are subject to hostile disruption through solely virtual means. A recent Draft Report of the Chair of the COPOUS Working Group on the Status and Application of the Five United Nations Treaties on Outer Space raised the question of expanding the scope of states' international responsibility and liability under this Convention [40]. The European Union's 2014 Draft Code of Conduct also formulates a broad approach, advocating "…the freedom for all States, in accordance with international law and obligations, to access, to explore, and to use outer space for peaceful purposes without harmful interference, fully respecting the security, safety and integrity of space objects…" [41]. It specifically endorses improving states' adherence to, and implementation of, ITU regulations addressing harmful radio-frequency interference [42].

It is proposed here that a reasonable interpretation of Article VII might also include damage caused virtually by hostile disruption to satellite transmissions, whether by space debris or otherwise [43]. The Convention's concept of "loss or damage to property" would entail a determination that transmissions and the data they transmit constitute the "property" of a state or private entity the activity of which is attributable to a state. It is contended that this is not an unreasonable extension of the scope of the Convention, especially given the high commercial and financial value of many such transmissions. There is also precedent for such an approach, as in the application of the WIPO Convention to satellite transmissions, which it views as assets capable of bearing proprietary rights [44]. Moreover, commercial satellite operators and satellite consortia, such as International Maritime Satellite Organization (IMSO), are bound to provisions within their conventional regimes that require compensation when client transmissions are interrupted, distorted or otherwise damaged [45].

In summary, the application of space law to the disruption of satellite transmissions may be characterized as follows. The determinative point of departure for space law is general international law, including the UN Charter and its regime of collective security. Although states may not claim sovereignty over particular territories in outer space, including the moon and other celestial bodies, satellites do remain under the sovereignty and the responsibility of the launching state or states. These legal principles are established in the OST, which also provides (together with the Liability Convention) for the liability of states for damage caused by satellites throughout the satellite's life span. In this author's view, the definition of "damage", crucial to the application of the Liability Convention, may be understood to include injuries caused by either kinetic or virtual means, including damage caused through and in cyberspace. More controversial is the question of whether satellite transmissions may be considered "property" under the Liability Convention, together with the applicable commercial satellite agreement, and are covered by its provisions. It is proposed that certain satellite transmissions are in fact subject to the Liability Convention as "property" and are protected by its provisions. Nonetheless, state practice regarding the issue is currently lacking, as it is, to a lesser degree, regarding liability for the clearer case of physical damage to satellites [46].

3.3. International telecommunications law

This field of international telecommunications law has been developed largely under the aegis of the leading inter-governmental organization in the field, the International Telecommunications Union (ITU). The ITU is also the UN specialized agency charged with the global regulation of telecommunications. The ITU Constitution, currently ratified by 193 Member States, defines "telecommunication" as "Any transmission, emission or reception of signs, signals, writing, images and sounds or intelligence of any nature by wire, radio, optical or other electromagnetic systems [47]. This broad, technology-neutral definition encompasses satellite and other types of communications that utilize both wireless and wired networks; on the earth, in the atmosphere, and in outer space.

The organization's Radiocommunications Sector (RS) assigns orbital slots and coordinates to satellites through its Space Services Department and maintains the relevant portion of the Master International Frequency Register (MIFR) [48] relating to satellite registration by country, uplink and downlink frequency assignments, orbital location, and satellite expiry date [49]. In carrying out the implementation of satellite registrations and regulation of their use, the ITU and its member states are bound by several substantive principles included in its instruments (Constitution, Convention and Telecom and Radio Regulations) that apply to the global use of telecommunications infrastructure such as undersea cables, microwave connections and satellite systems [50].

The first relevant principle is embodied in Article 33 of the ITU Constitution, and establishes the non-discriminatory use of "the international service of public correspondence" [51], including relevant satellite communications. Articles 34 and 35, entitled "Stoppage of Telecommunications" and "Suspension of Services", affect and counterbalance this right by permitting Member States to suspend ingoing and outgoing telecommunications, including those transmitted by satellite, with respect their own territory, on the condition that they publicly notify the stoppage or suspension as stipulated [52]. These authorities stems from a state's capacity as a sovereign to control the flow of information through its territory, yet does not extend beyond its borders other than in exceptional situations [53].

Two additional ITU Constitutional provisions are relevant to the context of satellite transmissions. Article 44 provides that the global electro-magnetic spectrum resource and the geostationary satellite orbit are limited natural resources that must be used "rationally, efficiently and economically" and that "…countries or groups of countries [must] have equitable access to those orbits and frequencies…." [54] This provision establishes an

internationally-agreed characterization of the spectrum and orbits that has legal ramifications for the provision of transmission uplinks and downlinks, for instance.

Finally, and most significantly for the present topic, Article 45 of the Constitution prohibits the disruption of all wireless communications, including satellite transmissions, from "harmful interference". This key term is defined in detail by Article 15 of the ITU Radio Regulations, and prohibits "…unnecessary transmissions, or the transmission of superfluous signals, or the transmission of false or misleading signals, or the transmission of signals without identification" [55]. It is also worth noting that emergency communications are given special protection by the subsequent Article 46, and receive "absolute priority" [56] over other types of telecommunications.

The ITU Constitution's exemption of military installations, including military satellite installations, from the two latter normative provisions does complicate the application of the ITU legal regime across all satellite system infrastructures [57], especially given the dual-use nature of contemporary satellite systems [58]. The difficulties of separating out the military and civilian uses of a particular satellite present a challenge at the practical and legal level that has yet to be resolved [59].

To summarize the ITU regulatory regime as it applies to satellite networks and communications, the ITU constitutional provisions provide a relatively clear, robust and widely-accepted normative and regulatory position that supports and facilitate uninterrupted satellite communications. Moreover, the ITU norms specifically prohibit harmful interference with transmissions, and require states to operate with transparency regarding any interruptions to the satellite communications of other states. These provisions are rooted in a long-standing treaty regime that has developed over the course of the evolution of wireless communications since the 19th century, and to which nearly all states are bound at present [60].

3.4. *Transborder freedom of information*

The fourth international legal regime relevant to the protection of satellite transmissions is that of the freedom of transborder information flow. This regime deals with content-related aspects of communications, rather than the technical aspects that are more characteristic of the preceding two regimes of space law and international telecommunications law.

The transborder freedom of information is recognized under international law by both treaty law and customary law. It is concisely formulated in Article 19 of the Universal Declaration of Human Rights, as follows:

> "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers" [61].

This broad formulation is technology-neutral by intent, and applies to satellite communications just as it applies to printed newspapers and to letters sent through the post. It is supported by customary law with a history associated with the development of the 19th century's Western concepts of democracy and freedom of expression [62]. One early effort to restrict transborder freedom of information exchange, by excluding hostile propaganda and incitement to war, was promoted in the1936 International Convention Concerning the Use of Broadcasting in the Cause of Peace [63]. This treaty, acceded to by about 30 countries, attempted to respond to public incitement to war via radio broadcasting during WWI. Article 1 of the Convention, for instance, requires states to prohibit broadcast transmissions within their territories that are "of such a character as to incite the population of any territory to acts incompatible with the internal order or the security of a territory". Throughout World War II, during the Nuremberg Trials, and for the duration of the Cold War, the question of whether states are permitted under international law to jam propaganda broadcasts from hostile states was debated by international lawyers. In the post-War period, the debate was carried out in the context of dozens of UN and UN specialized agency decisions and resolutions, on occasion focusing on the alleged distortion of the developing world on the part of the media owned and run by the so-called first world [64]. The legal debate was further carried over during the 1970s into the realm of direct broadcast satellite transmissions (DBS) and the "free flow versus prior consent" argument [65].

Domestic law provisions that set out the parameters of the freedom of communications and the limitations on its scope are critical to its application to satellite communications, as are further provisions of international law [66]. One important aspect of the debate over prohibited content as an exception to the rule supporting transborder freedom of information exchange is analyzed in a 1997 article by Jamie Metzl reviewing the legality of the 1994 RTLM radio broadcasts that were eventually determined by the International Criminal Trial for Rwanda (ICTR) to constitute incitement to genocide of the Tutsi. The ICTR determined that the Hutu management personnel of the RTLM radio station held personal responsibility for violating norms of *jus cogens* [67]. In the article, Metzl evaluates the applicable customary law:

> "…stripped of its Cold War overtones, the international law regarding radio jamming is not nearly as uniform and absolute as it may once have seemed, even if the strong presumption toward the free flow of information and against jamming continues to fulfill a valuable international role" [68].

Metzl thus argues that there are limitations to the above-mentioned Article 19 freedom of communication that would ostensibly prohibit disruption of radio broadcasts in another state's territory. The Rwanda broadcasts inciting to genocide may have legitimately been jammed, in his view – there may even be a duty to jam broadcasts that violate *jus cogens*. This conclusion finds some support in UN Charter Article 41, which permits the Security Council to require states to interrupt "postal, telegraphic, radio and other means of communication" as a response to a threat to peace, danger to peace or aggression [69].

In extending this conclusion into the context of satellite transmissions, international law does recognize limitations on the international freedom of transborder communication, including satellite transmissions. This freedom may be curtailed by domestic law provisions, such as those addressing national security issues [70]; by the Security Council acting under Article 41; and possibly by *jus cogens* considerations (i.e., to prevent incitement to genocide). Overall, the impact of extending freedom of communication into cyberspace requires the engagement of new modes of thinking about the normative framing, the practice and the enforcement of this international human right [71].

4. Towards a framework for cooperation under international law

The convergence of the four regimes of international law reviewed above around the issue of hostile disruption of satellite communications provides an opportunity to test the viability of international law as it relates to a rapidly-developing phenomenon of state activity of concern to many countries and international organizations. Yet the provision of a clear legal solution available

to victim states, i.e., states that have undergone hostile disruption to their satellite communications, whether physically, virtually or in some hybrid combination, is still unresolved [72].

Additionally, it is unclear how the international law applicable in cyberspace, although not yet developed or sufficiently elucidated by state practice, will influence the application of these four regimes. The intersections of this field of law with the four reviewed in this article will be salient and interesting to observe as states forge new norms of behavior, adapting existing international law norms to cyberspace.

Nonetheless, the need to explore and connect cybersecurity considerations and emerging legal norms with these more established fields of law continues to be under-prioritized: a recent COPOUS proposal on space governance does not refer to cybersecurity issues, for instance; nor does the April 2016 Draft Report of the Chair of the Working Group on the status, application and enforcement of the five space treaties [73]. Issues of the applicability of international law to outer space and to cyberspace appear to be "siloed" at present.

This article proposes that a comprehensive and integrative multi-stakeholder review of the measures available under international law in response to hostile acts directed at satellites and satellite transmissions be undertaken with some urgency. Indeed, the 2013 GGE noted that "…efforts by States, and the international community as a whole, are being undertaken to advance concerted, well-thought out, effective and timely bilateral, regional and multilateral initiatives to strengthen stability and security in outer space in a constructive manner" [74]. Yet the relevance of cybersecurity concerns has not, on the whole, been integrated into these efforts.

In this author's view, a dedicated framework for cooperation among states and relevant non-state actors, such as commercial satellite corporations, is called for, with due consideration of the rapid development of cyber-enabled ASAT capabilities and threats by state and non-state actors, as well. The typology of hostile satellite disruptions proposed in this article may serve as an analytical matrix for triggering the appropriate international law responses to hostile interference with satellites and satellite transmissions.

5. Conclusions

The underlying assumption of this article is that international law has a key role to play in articulating the "rules of the road" for state activities relating to satellites, including the imposition of effective sanctions on those states that do not uphold and implement applicable legal norms. The additional, relatively new issue of the application of international law to state and non-state activities in cyberspace is a factor that also needs to be considered when weighing the range of possibilities for state responses to hostile disruptions to satellite communications. This article proposes a typology of hostile satellite events and reviews the four relevant legal regimes as well as the relevance of cybersecurity considerations and nascent norms. It urges the establishment of a global framework for effective multi-stakeholder cooperation under international law in responding to kinetic, virtual and hybrid threats to satellite communications of all types and clarifying the applicable norms of responsibility and liability in this context.

References

[1] G. Leopold, Russian hacker group taps satellite links for attacks, Defense Systems, September 10, 2015, ⟨https://defensesystems.com/articles/2015/09/10/turla-apt-group-satellite-link-hacks.aspx⟩.

[2] C. Baraniuk, "GPS errors caused '12 hours of problems' for companies", BBC News, 4 February 2016. North Korea has also threatened to disrupt South Korean GPS signals since 2010, on various occasions ("S. Korea preparing for NK GPS disruption", Yonhap News Agency, February 19, 2016).

[3] See also "Hacking Satellites: Look Up to the Sky", InfoSec, September 18, 2013.

[4] (a) See Union of Concerned Scientists Satellite Database, updated through December 31, 2015, ⟨http://www.ucsusa.org/nuclear-weapons/space-weapons/satellite-database.html#.VgQDWcub7IU⟩.
(b) The procedures for satellite filings with the International Telecommunications Union's Radiocommunication Bureau in ITU-R, Performance Report for 2013, Geneva, 2014. In this context, satellite orbits include geosynchronous orbit, 35,786 km above sea level, as well as several other orbital levels.

[5] (a) See presentation by R. Levi, T. Dekel, Space Security: National Capabilities and Programs, United Nations Institute for Disarmament Research, April 2011.
(b) L. Perek, Space debris mitigation and prevention: how to build a stronger international regime, Astropolitics 2 (2004) 215–226.

[6] (a) M. Zenko, Dangerous Space Incidents, Council on Foreign Relations, April 2014.
(b) C. Baylon, Challenges at the Intersection of Cyber Security and Space Security, Chatham House, United Kingdom, 2014.

[7] See CNN, UN Security Council condemns North Korean rocket launch, ⟨http://edition.cnn.com/2016/02/07/asia/north-korea-rocket-launch-window/⟩.

[8] S. Clark, Iranian Satellite Successfully Placed in Orbit, Spaceflight Now, February 2, 2015.

[9] A. Shalal-Esa, U.S. sees China launch as test of anti-satellite muscle, Reuters, May 13, 2015.

[10] (a) See D. Kestenbaum, Chinese Missile Destroys Satellite in 500-mile Orbit, January 19, 2007, ⟨http://www.npr.org/templates/story/story.php?storyId=6923805⟩.
(b) U.S. Shoots Down Toxic Satellite, Daily Telegraph, February 20, 2008.;
(c) D. Housen-Couriel, Satellite Wars are Coming Next, Jerusalem Post, February 14, 2007.

[11] World Economic Forum, Risk and Responsibility in a Hyperconnected World: Pathways to Global Cyber Resilience, 2012.

[12] (a) See "Defending the Networks: The NATO Policy on Cyberdefense", October 4, 2011.
(b) Council of the European Union (2005), Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems, OJ L 69, 16.3.2005, p. 67.
(c) Council of the European Union (2008), and Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, OJ L 345, 23.12.2008, p. 75.

[13] Zenko, supra note 6. See also "GPS Jamming: Out of Sight", The Economist, July 27, 2013.

[14] The UN Secretary-General noted in his Foreword to the Report that "Satellites provide strategic advantages but they are also vulnerable. Protecting space assets has thus become a serious international security concern." See Report of the Group of Governmental Experts ("GGE Report"), A/68/189, 27 September 2013, at 4. See also Baylon, supra note 6.

[15] GGE Report, ibid; and the European Union Draft International Code of Conduct for Outer Space Activities ("European Draft Code of Conduct"), 31 March 2014, at #25, ⟨http://www.eeas.europa.eu/non-proliferation-and-disarmament/pdf/space_code_conduct_draft_vers_31-march-2014_en.pdf⟩.

[16] Baylon, supra note 6.

[17] See supra note 3.

[18] E. Conrad et al., Collateral Damage to Satellites from an EMP Attack, Defense Threat Reduction Agency, US STRATCOM, August 2010.

[19] See, Eutelsat condemns jamming of broadcasts from Iran and renews appeals for decisive action to international regulators, 4 October 2012, ⟨http://www.eutelsat.com/home/news/press-releases/Archives/2012/press-list-container/eutelsat-condemns-jamming-of-bro.html⟩.

[20] Baylon, supra note 6.

[21] (a) See, for instance, the Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, June 26, 2015.
(b) M. Schmitt (Ed.), Tallinn Manual on the International Law Applicable to Cyber Warfare ("Tallinn Manual")Cambridge University Press, Cambridge, 2013.

[22] Baylon, supra note 6, at 5.

[23] The applicability of the collective security regime in outer space is reviewed below, in the context of the OST.

[24] (a) Physical attacks on satellites are dealt with under the space law conventions. General international law considerati ons, such as due attribution, will apply to analysis of particular attacks.
(b) M. Bourbonniere, Law of armed conflict (LOAC) and the neutralisation of satellites, or *ius in bello satellitis*, J. Confl. Secur. Law 9 (2004).

[25] "[S]pace operations are entirely cyberspace dependent. In other words, space capabilities cannot be employed without cyberspace." J. Robinson, "Governance challenges at the intersection of space and cybersecurity", The Space Review, February 15, 2016.

[26] Tallinn Manual, supra note 21.

[27] The Tallinn Manual and the latest version of the United Nations Group of

Government Experts (GGE) engage with these questions and determine that the Charter regime is generally applicable in cyberspace. See Tallinn Manual, ibid, and Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, supra note 21.

[28] (a) In particular, issues of state sovereignty, military necessity, distinction between combatants and non-combatants, and attribution are currently at the core of debate among international legal scholars.
(b) M. Schmitt, L. Vihul, The emergence of legal norms for cyber conflict, in: Fritz Allhoff (Ed.), Binary Bullets: The Ethics of CyberwarfareOxford University Press, Oxford, 2014.

[29] The 2008 Draft Treaty on Prevention of the Placement of Weapons in Outer Space and of the Threat or Use of Force against Outer Space Objects, proposed by the Russian Federation and China, defines the use of force or its threat as "…"any hostile actions against outer space objects including, inter alia, actions aimed at destroying them, damaging them, temporarily or permanently disrupting their normal functioning or deliberately changing their orbit parameters, or the threat of such actions.(Letter dated 12 February 2008, UNODA Conference on Disarmament, CD/1839, 29 February 2008.

[30] See for instance, M. Schmitt, "Rewired Warfare: Rethinking the Law of Cyber Attack", 96 International Review of the Red Cross, 2014.
(b) T. Wingfield, Legal aspects of offensive information operations in space, USAF Acad. J. Legal Stud. 9 (1998/99) 121.
(c) Bourbonniere, supra note 24.
(d) K. Schendzielos, "Electronic Combat in Space: Examining the Legality of Fielding a Space-Based Disruptive Electromagnetic Jamming System", Master's Thesis, Army Command and General Staff College, Fort Leavenworth, Kansas, 15 June 2007. On the addition of a relevant fifth domain (cyberspace) to the traditional four domains of warfare (land, sea, air, space), see "War in the Fifth Domain" The Economist, July 1, 2010; and NATO, NATO 2020: Assured Security; Dynamic Engagement, May 17, 2010.

[31] One definition of such "critical infrastructure" is that included in Article 2(a) of the 2008 EU Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (Official Journal of the European Union, L345/75). See, as well, the 2012 Commission Staff Working Document which reviewed its implementation.

[32] For the status of the 1967 Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies (London, Moscow and Washington D.C., January 27, 1967) and other space law treaties, see UN Office for Outer Space Affairs, Status of International Agreements relating to activities in outer space as at 1 January 2015, 8 April 2015 (A/AC.105/C.2/2015/CRP.8*). For review and analysis of the law of space as it relates to satellites, see N. Jasentuliyana, "A Survey of Space Law as Developed by the United Nations", in Perspectives on International Law, (ed. N. Jasentuliyana), Kluwer, 1995.

[33] See UNOOSA Draft Report, A/AC.105/C.2/2016/TRE/L.1, 12 April 2016.

[34] The Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, UNGA Resolution 2222 (XXI), 1966. As of October 2011, 100 countries (including Israel) are parties, while another 26 have signed but have not completed ratification.

[35] See UNOOSA, Space Law Treaties and Principles, ⟨http://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties.html⟩.

[36] "Outer space, including the Moon and other celestial bodies, is not subject to national appropriation by claim of sovereignty, by means of use or occupation, or by any other means" (Article II, ibid).

[37] Article VI determines that "the activities of non-governmental entities in outer space, including the Moon and other celestial bodies, shall require authorization and continuing supervision by the appropriate State Party to the Treaty", and that Parties bear international responsibility for national space activities carried out by either governmental or non-governmental entities.

[38] The Convention on International Liability for Damage Caused by Space Objects, UNGA Resolution 2777 (XXVI), 1971. Two additional treaties address additional aspects of states' responsibility regarding satellites and their use: The Convention on Registration of Objects Launched into Outer Space (UNGA Resolution 3235 (XXIX), November 12, 1974); and The Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space (UNGA Resolution 2345 (XXII), December 19, 1967).

[39] Article I, Liability Convention, ibid. See J. Hermida, "International Space Law", in Legal Basis for a National Space Legislation, Kluwer, 2004; and M. Listner, "Revisiting the Liability Convention: reflections on ROSAT, orbital space debris, and the future of space law", The Space Review, October 17, 2011.

[40] See Report of the Chair of the Working Group on the Status and Application of the Five United Nations Treaties on Outer Space (in the annexed proposed questions), 12 April 2016, A/AC.105/C.2/2016/TRE/L.1.

[41] European Draft Code of Conduct, supra note 15.

[42] Ibid, at #53.

[43] See also the analysis of "damage" in E. Carpanelli and B. Cohen, "Interpreting 'Damage Caused by Space Objects' under the 1972 Liability Convention", IAC-13, at ⟨http://www.iislweb.org/docs/Diederiks2013.pdf⟩.

[44] See "Technological and legal developments in intellectual property", Chapter 7, in: WIPO Intellectual Property Handbook: Policy, Law and Use, pp. 451–453.

[45] IMSO Convention and LRIT Agreement, see ⟨www.imso.org⟩.

[46] (a) See Settlement of Claim between Canada and the Union of Soviet Socialist Republics for Damage Caused by Cosmos 954, April 2, 1981, ⟨http://www.jaxa.jp/library/space_law/chapter_3/3-2-2-1_e.html⟩.
(b) E. Galloway, Nuclear powered satellites: the U.S.S.R. Kosmos 954 and the Canadian Claim, Akron Law Rev. 12 (1979) 401.

[47] ITU Constitution, Annex, ⟨http://www.itu.int/en/history/Pages/ConstitutionAndConvention.aspx⟩, 1012.

[48] See Space Plan Assignments Recorded in the ITU's Master International Frequency Register ("MIFR").

[49] The ITU provides extensive information on the MIFR and the regulatory processes applicable to satellites. See the ITU website ⟨www.itu.int⟩ and, for instance, Y. Henri, "Satellite International Regulatory Framework: Added Value or Hindrance to Development", ITU-R, 3–4 February 2010.

[50] See the recent controversy around Egypt's request to extend the launch deadline of the satellite Navisat 12-A, citing "force majeure" (P. DeSelding, "Officials fear precedent set as Egypt wins ITU satellite approval pleading 'force majeure'", SpaceNews, February 11, 2016).

[51] Member States recognize the right of the public to correspond by means of the international service of public correspondence. The services, the charges and the safeguards shall be the same for all users in each category of correspondence without any priority or preference. ITU Constitution, supra note 47, Article 33.

[52] ITU Constitution, ibid.

[53] In fact, the opposite is the case: under Article 38, states are required to ensure optimal technical conditions for uninterrupted international telecommunications, and to refrain in particular from disrupting operations in other states.

[54] Ibid.

[55] ITU Radio Regulations, ⟨http://www.itu.int/en/ITU-R/terrestrial/tpr/Documents/Article15-RR12.pdf⟩, 2012.

[56] Radio stations shall be obliged to accept, with absolute priority, distress calls and messages regardless of their origin, to reply in the same manner to such messages, and immediately to take such action in regard thereto as may be required. (ibid).

[57] Article 48, ibid.

[58] The difficulty of defining a 'space weapon' is compounded by the potential for almost any space object to be used as a weapon in space. For example, a civilian satellite (e.g. for weather monitoring) could effectively be turned into a weapon (Baylon, supra note 6, p. 11).

[59] J. Del Rosario, C. Rousseau, An Analysis of Hosted Payloads and Dual-use Satellites as Middle Ground between Commercial Outsourcing and Internal Asset Deployment, Northern Sky Research, no date ⟨http://www2.isunet.edu/index2.php?option=com_docman&task=doc_view&gid=762&Itemid=26⟩.

[60] The provisions on uninterrupted communications over the electro-magnetic spectrum were included in the early, mid-19th century versions of the ITU Constitution.

[61] UNGA 217 A (III) 1949. Article 29 potentially tempers the scope of Article 19 and other rights set forth in the Declaration by prescribing "respect for the rights and freedoms of others" and the requirement of "meeting the just requirements of morality, public order and the general welfare".

[62] See P. Malancuk, Information and communication, freedom of, in: R. Bernhardt, et al., (Eds.), Encyclopedia of International Law, 9, North-Holland, Amsterdam, 1986, p. 148.

[63] Signed on September 23, 1936, LNTS Vol. 186, p. 301.

[64] (a) J. Whitton, Cold war propaganda, Am. J. Int. Law 45 (1951) 151.
(b) J. Metzl, Rwandan genocide and the international law of radio jamming, Am. J. Int. Law 91 (1997) 628 (636–645).
(c) D. Housen-Couriel, International telecommunications law and international cyber law, in: R. Sabel (Ed.), International Law, 3rd ed.,Sacher Institute, Jerusalem, 2016.

[65] J. Savage, M. Zacher, Free flow vs. prior consent: the jurisdictional battle over international telecommunications, Int. J. 42 (1987) 342.

[66] See Article 29 of the Universal Declaration on Human Rights, supra note 61.

[67] Prosecutor v. Ferdinand Nahimana et al., Case No. ICTR-99–52-T, 3 December 2003.

[68] Metzl, supra note 64, at 650.

[69] The Security Council may … call upon the Members of the United Nations to apply such measures [as] complete or partial interruption of …postal, telegraphic, radio, and other means of communication.

[70] On the balancing of these considerations see, for instance, the Global Principles on National Security and the Right to Information ("The Tshwane Principles"), Open Society Justice Initiative, June 12, 2013, ⟨https://www.opensocietyfoundations.org/publications/global-principles-national-security-and-freedom-information-tshwane-principles⟩.

[71] See, for instance, V. Nash, Analyzing freedom of information online: theoretical, empirical and normative contributions, in: W. Dutton (Ed.), The Oxford Handbook of Internet Studies, Oxford, 2013.

[72] See, for instance, C. Jolly, An OECD View: The Growing Risks of Satellite Signal Interference, in Baylon, supra note 6, p. 44.

[73] COPOUS, Updated proposal for a UNISPACE+50 thematic priority to be considered by the Legal Subcommittee, 11 April 2016 (A/AC.105/C.2/2016/CRP.20); UNOOSA Draft Report, supra note 30.

[74] GGE Report, supra note 14, p. 10.