Cybersecurity and Anti-Satellite Capabilities (ASAT): New Threats and New Legal Responses

Deborah Housen-Couriel, LL.M., Adv.*

INTRODUCTION: FRAMING THE LEGAL ISSUES

The sophisticated hacking of satellite communications by the so-called Turla group, characterized by one media source as "a Russian-speaking spy gang", has recently received broad publicity as an example of a new type of hostile cyber capability.[1] The Turla hackers exploited

* Deborah is an independent legal and policy expert in four major areas of Israeli and global cybersecurity and regulation: cyber defense and readiness, critical infrastructure protection, cyber terrorism and internet governance. She researches, writes and speaks frequently on these issues at academic and professional conferences. Deborah is a member of the Israeli Bar Association and Special Counsel to the New York law firm Zeichner, Ellman and Krause LLP in the field of cybersecurity. Currently, she is a member of the International Group of Experts drafting the "Tallin 2" manual on state activity in cyberspace; and of the ILA's Study Group on Cybersecurity, Terrorism and International Law. In 2010-11, she co-chaired the National Cyber Initiative Policy and Regulation Committee, under the aegis of the Prime Minister's Office. She works closely with Konfidas Digital, a leading Israeli cybersecurity firm.

[1] *See* Kim Zetter, *Russian Spy Gang Hijacks Satellite Links to Steal Data*, WIRED (Sept. 9, 2015), http://www.wired.com/2015/09/turla-russian-espionage-gang-hijacks-satellite-connections-to-steal-data/; George Leopold, *Russian hacker group taps satellite links for attacks*, DEFENSE SYSTEMS (Sept. 10, 2015), https://defensesystems.com/articles/2015/09/10/turla-apt-group-satellite-link-hacks.aspx).

vulnerabilities in satellite uplinks and downlinks that connected with compromised ISP servers, and took advantage of existing IP addresses in order to extract data from malware-infected computers without identification of the associated command server. The exploit has allowed for the anonymous hacking of hundreds of government and corporate computers in nearly 50 countries. In exposing the group's most recent hacks, Kaspersky experts described its technique as "exquisite" because of its effectiveness in ensuring anonymity by disguising the command server's identity.[2] An additional advantage of the Turla hackers' *modus operandi* is the wide area of vulnerability provided by the broad geographical area covered by satellite footprints (see Figure 1).

As cutting-edge as the Turla hack appears, it is in fact old news in the context of the hostile interruptions of satellite communications. This particular group has allegedly been active since 2007, and other groups have utilized similar techniques for decades, to distort, jam, modify and otherwise exploit satellite uplinks and downlinks.[3]

---

[2] Horia Ungureanu, *Russian Hackers Hijack Satellites to Steal Data From Governments, Military, And Other Organizations*, TECH TIMES (Sept. 10, 2015), http://www.techtimes.com/articles/83504/20150910/russian-hackers-hijack-satellites-to-steal-data-from-governments-military-and-other-organizations.htm.

[3] "Abuse of satellite links is not solely the domain of Turla. HackingTeam command and control servers, for example, were found to be using such links to mask operations, as were links traced to Rocket Kitten and Xumuxu, two APT groups that are government-backed or have governments as customers…" Michael Mimoso, *Turla APT Group Abusing Satellite Internet Links*, THREATPOST (June 11, 2015), https://threatpost.com/turla-apt-group-abusing-satellite-internet-links/114586/.

States, as well as non-state actors, have taken advantage of Turla-type exploits. Yet the strategic legal and policy issues raised by the intersection of cybersecurity vulnerabilities and other anti-satellite capabilities (ASAT) have not until now been sufficiently addressed by space-faring countries and organizations.

This lack of attention on the part of practitioners and scholars is due, to a certain extent, to the ongoing *de facto* freedom of activity in cyberspace which states continue to reserve for their own offensive and defensive activities.[4] This article argues that the *lacuna* regarding cyber-mediated ASAT, until now, is also a result of two additional phenomena that stem from its legal complexities. The first is the nexus of the four legal regimes that presently apply to the hostile interruption of satellite communications. The second is the need to re-frame each of these regimes and the nexus they constitute in the context of developing legal norms applicable to state activity in cyberspace, the domain in which satellite communications take place.[5] These two

[4] *See*, Bill Chappell, *Obama: Cyberspace is the New 'Wild West'*, NPR (Feb. 13, 2015), http://www.npr.org/sections/thetwo-way/2015/02/13/385960693/obama-to-urge-companies-to-share-data-on-cyber-threats; Jeremy Fleming, *Cyber security directive held up in face of 'Wild West' internet*, EurActiv (Apr. 1, 2015), http://www.euractiv.com/sections/infosociety/cyber-security-directive-held-face-wild-west-internet-313431).

[5] Michael Schmitt, *Introduction*, *in* RESEARCH HANDBOOK ON INTERNATIONAL LAW AND CYBERSPACE 1-9 (Nicholas Tsagourias & Russell Buchan eds., 2015); Nicholas Tsagourias, *The Legal Status of Cyberspace*, *in* RESEARCH HANDBOOK ON INTERNATIONAL LAW AND CYBERSPACE 13-29 (Nicholas Tsagourias & Russell Buchan eds., 2015).

legal challenges are the focus of the present analysis.

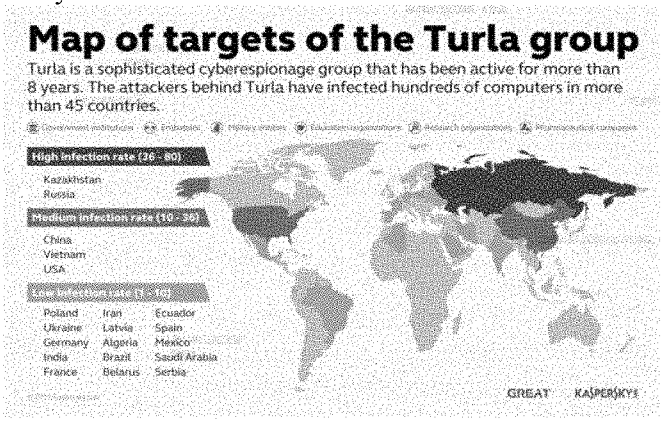

Figure 1: Kaspersky Labs, 2015.

I. SATELLITES AND CYBERSPACE

The potential for the disruption of satellite transmissions exists during all phases of a satellite's lifespan: the pre-launch testing phases, the launch itself, the satellite's active phase, and ending with its de-activation. Hostile disruptions are technically feasible by both kinetic and cyber means. Examples include the direct collision of one satellite with another with an intent to disable, jamming of transmissions with intent to block, distortion of the transmission, morphing, and aiming an electro-magnetic pulse (EMP) with intent to damage the satellite.[6] It is important to note at the outset that disruptions may also occur through error or negligence, i.e. without hostile intent – these events

[6] Edward Conrad et al, *Collateral Damage to Satellites from an EMP Attack*, DEFENSE THREAT REDUCTION AGENCY (Aug. 2010), http://www.dtic.mil/get-tr-doc/pdf?AD=ADA531197.

are not the subject of the present analysis, although they may entail liability under international and domestic law.[7]

As we shall see herein, the legal ramifications of hostile disruptions are not restricted to the technical aspects of the disruption. When the aim of the disruption is to influence or block particular content, the international law regime governing freedom of information across borders may come into play.[8] Examples include the 2007 Tamil Tigers rebel group substituting an Intelsat satellite broadcast of the Sri Lankan government with its own propaganda broadcast;[9] and Iran's disruption of Eutelsat transmissions including BBC Persian, the VOA Persian service and Radio Free Europe's Radio Farda.[10]

A. DEFINITIONS OF CYBERSPACE

---

[7] For a proposed typology of hostile disruptions, *see* Deborah Housen-Couriel, *Cybersecurity Threats to Satellite Communications: Towards a Typology of State Actor Responses*, PROC. OF THE 66TH INT'L ASTRONAUTICAL CONG. (2015).

[8] The present scope of the regime does not provide absolute assurance of the right to transmit all content. *See infra* at notes 58-61.

[9] Jill Stuart, *Satellite industry must invest in cyber security*, FINANCIAL TIMES: CYBERSECURITY (Apr. 10, 2015), http://www.ft.com/cms/s/0/659ab77e-c276-11e4-ad89-00144feab7de.html#axzz3vdcYQzzs.

[10] *See* Press Release, Eutelsat, Eutelsat condemns jamming of broadcasts from Iran and renews appeals for decisive action to international regulators (Oct. 4 2012), *available at* http://www.eutelsat.com/home/news/press-releases/Archives/2012/press-list-container/eutelsat-condemns-jamming-of-bro.html

In order to analyze the relevant legal regimes which govern satellite-disruptions in cyberspace, the parameters of this new realm of human activity first need to be defined. An agreed definition of cyberspace in the context of public international law is still developing; nonetheless, certain elements are consistently present in the various definitions that have so far been proposed.[11] For instance, the 2013 Tallinn Manual on the International Law Applicable to Cyber Warfare (herein, "Tallinn Manual") defines cyberspace as "[t]he environment formed by physical and non-physical components, characterized by the use of computers and the electro-magnetic spectrum, to store, modify and exchange data using computer networks."[12] In the US Department of Defense's Dictionary of Military Terms, cyberspace is defined as "[a] global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[13] Finally, Israel's government has defined cyberspace as "…the physical and non-physical domain that is created or composed of part or all of the following components: mechanized and computerized systems, computer and communications networks,

[11] Tsagourias, supra note 5.

[12] MICHAEL SCHMITT (ED.), TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (2013). (herein, "Tallinn Manual), p. 279.

[13] Approved for inclusion in the general glossary for Joint Doctrine. *See Cyberspace,* DOD DICTIONARY OF MILITARY TERMS (Oct. 15, 2015), *available at* http://www.dtic.mil/doctrine/dod_dictionary/data/c/10160.html.

programs, computerized information, content conveyed by computer, traffic and supervisory data and those who use such data."[14]

In general, these and other definitions of cyberspace encompass three basic elements: computers, the transmission networks connecting them (both wired and wireless), and the data stored in, processed by and transmitted through them.[15] For the purposes of the present analysis, satellite communications almost always take place in cyberspace: they are transmitted between earth stations (wired and wireless), between satellites (wireless), and via uplinks and downlinks (wireless).[16] Moreover, it is important to clarify that communication through cyberspace is by no means restricted to utilization of internet communications protocols. All communications formats that are used for satellite transmissions and for transmissions between ground stations are relevant to the analysis of the international law applicable to ASAT, as they meet the underlying criteria of data communications that take place through computer systems, operating as elements of cyberspace.[17]

---

[14] Israel Government Resolution 3611, Advancing National Cyberspace Capabilities (Aug. 7, 2011), *available at* http://www.pmo.gov.il/English/PrimeMinistersOffice/DivisionsAndAuthorities/cyber/Documents/Advancing%20National%20Cyberspace%20Capabilities.pdf_.

[15] Some definitions also specify software and personnel.

[16] Transmissions within the satellite itself or within specific computers are not unanimously considered communications through cyberspace.

[17] *See* GÉRARD MARAL & MICHEL BOUSQUET, *Satellite Networks*, *in* SATELLITE COMMUNICATIONS SYSTEMS: SYSTEMS, TECHNIQUES AND TECHNOLOGIES (5th ed., 2009).

II. ANTI-SATELLITE CAPABILITIES (ASAT): THE NEW THREAT ENVIRONMENT

ASAT encompass both physical and virtual or cyber threats to the more than 1,000 satellite systems currently in orbit,[18] launched by over 70 space agencies located in 60 countries.[19] ASAT relating specifically to satellite communications is rapidly developing in the context of hostile state capabilities in outer space, including activities carried out on space objects. The legal regime applicable to hostile activities in outer space in general is beyond the scope of this present paper, but is nevertheless important for a full understanding of the legal regimes analyzed below.[20]

A. KINETIC ASAT

---

[18] *See* UNION OF CONCERNED SCIENTISTS SATELLITE DATABASE, http://www.ucsusa.org/nuclear-weapons/space-weapons/satellite-database.html#.VgQDWcub7IU (last updated Aug. 31, 2015)., and 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.

[19] Thirteen of these states possess independent launching capability. These states are (in order of their independent launches) Russia (USSR), US, France, Japan, China, UK, India, Israel, Ukraine, Russia, Iran, North Korea, and South Korea.

[20] On the current state of space law, *see* Jinyuan Su, *Space Arms Control: Lex Lata and Currently Active Proposals*, Asian J. of Int'l L., (Nov. 2015), *available at* CJO2015. doi:10.1017/S2044251315000223.

Kinetic ASAT relates to the physical destruction of satellite communications operations, in contrast to the exclusively virtual disruptions and the hybrid disruptions discussed below. One kinetic ASAT-related phenomenon involves states intentionally destroying their own satellites in order to demonstrate their potential ASAT capabilities. The idea is that if a state can destroy or physically impair one of its own satellites, those belonging to rival states are feasible targets. Recent events highlighting the physical vulnerability of satellites include the implementation or announcement by several states of satellite launches, long-range ballistic trials, space debris alerts and the like.[21] These include Iran's launch of the Fajr satellite in early 2015,[22] the North Korean satellite launch in December 2012, [23] the May 2013 launch by China of a research satellite into the ionosphere,[24] and the Russian launch of the Nudol anti-satellite missile in November 2015.[25] China and the US have each

[21] The potential dangers to satellites posed by increasing amounts of space debris is reviewed in Alexander Salter, *Space Debris: A Law and Economics Analysis of the Orbital Commons* (Mercatus Center Working Paper, September 25, 2015).

[22] Stephen Clark, *Iranian Satellite Successfully Placed in Orbit*, SPACEFLIGHT NOW (Feb. 2, 2015), http://spaceflightnow.com/2015/02/02/iranian-satellite-successfully-placed-in-orbit/.

[23] *North Korea Successfully Launches Satellite*, SPACE.COM (Dec.12, 2012), http://www.space.com/18867-north-korea-rocket-launch-satellite.html.

[24] Andrea Shalal-Esa, *U.S. sees China launch as test of anti-satellite muscle*, REUTERS (May 13, 2015), http://www.reuters.com/article/us-china-launch-idUSBRE94E07D20130516.

[25] L. Todd Wood, *Russia tests anti-satellite missile*, WASHINGTON TIMES (Dec. 2, 2015),

destroyed their own satellites (in 2007 and 2008, respectively), giving notice to the international community of their ASAT capabilities and their "willingness to engage" in this context.[26] Finally, the collision of a Russian Kosmos satellite with an iridium satellite in February 2009 will be discussed further below.

The utilization of kinetic ASAT capabilities may impact satellite communications in the most extreme way possible: physical destruction of a satellite or a ground station, or intentional and hostile dispersion of space debris, eliminating any possibility of continued communications by the satellite. Although the focus of the present analysis is cyber-mediated ASAT, the four international law regimes applicable to hostile disruptions also address in part the legal ramifications of kinetic ASAT, as we shall see herein.

B. VIRTUAL ASAT IN CYBERSPACE

---

http://www.washingtontimes.com/news/2015/dec/2/l-todd-wood-russia-tests-anti-satellite-missile/.

[26] *See* Brian Weeden, *Through a Glass Darkly: Chinese, American and Russian Anti-satellite Testing in Space*, THE SPACE REVIEW (Mar. 17, 2014); David Kestenbaum, *Chinese Missile Destroys Satellite in 500-mile Orbit* (Jan. 19, 2007), http://www.npr.org/templates/story/story.php?storyId=6923805; Catherine Elsworth & Richard Spencer, *Rogue satellite shot down over the Pacific*, THE TELEGRAPH (Feb. 21, 2008), http://www.telegraph.co.uk/news/worldnews/1579433/Rogue-satellite-shot-down-over-the-Pacific.html; and Deborah Housen-Couriel, *Satellite Wars are Coming Next*, JERUSALEM POST (Feb. 14, 2007), http://www.jpost.com/Opinion/Op-Ed-Contributors/Satellite-wars-are-coming-next.

The utilization of cyberspace has increased dramatically in recent years.[27] Hostile uses of cyberspace, including cybercrime, state-to-state hostile acts, terrorist use of the internet, electronic surveillance, and the establishment of data havens pose unprecedented threats to international stability. For example, the World Economic Forum has focused on cyber resilience as a response to the aggregation of these threats and exposures, resulting from the "hyperconnectivity" of contemporary economic, social, scientific, health, media, military and governmental functions.[28] In a January 2014 report, it explains the pervasiveness of this new threat environment: "Digital technology touches virtually every aspect of daily life today [....] the collective ability to manage cyber risks in this shared digital environment is fundamental. It forms the crux of cyber resilience."[29]

These exposures to the new cyberspace-based threat landscape are no less salient in the context of satellite communications.[30] Hostile disruption of these communications through cyberspace is being integrated into the strategic and tactical planning of states both in its defensive and offensive aspects,[31] and include jamming, morphing

---

[27] *See Risk and Responsibility in a Hyperconnected World*, WORLD ECONOMIC FORUM (Jan. 2014), *available at* http://www3.weforum.org/docs/WEF_IT_PathwaysToGlobalCyberResilience_Report_2012.pdf; ITU, MEASURING THE INFORMATION SOCIETY (2014).

[28] *Id.*

[29] *Id.*, at 5.

[30] Stuart, *supra* note 9.

[31] *See* Joint Chiefs of Staff, Joint Publication 3-14, *Space Operations*, US DEP'T OF DEFENSE (2014); Micah Zenko, *Dangerous Space Incidents*, Council on Foreign Rel. (Apr. 2014).

of signals, and other disruptions of computerized guidance, command and control, and communications systems.[32] In a hyper-connected world now characterized by the ubiquitous use of cyberspace,[33] non-kinetic or virtual disruption of satellite signals constitute an ongoing strategic and tactical threat to states. For instance, in the Joint Publication on space operations of the US Chiefs of Staff, the importance of cyber operations in space is emphasized:

> […] The physical domains (air, land, maritime, and space) and information environment rely on cyberspace for instant communications, but **the linkages between space and cyberspace are of particular importance** as space provides a global connectivity option for [cyber operations]. In addition, cyberspace provides the means by which space control and transmission of space sensor data are conducted. **These interrelationships are critical, and the linkages must be addressed during all phases of joint operation planning**.[34] (emphasis added)

Satellite communications now control critical national and global critical infrastructures such as military systems, banking and financial systems, air traffic control, electricity grids, traffic and transport systems, GPS, early-warning weather

---

[32] *See* presentation by Ram Levi & Tal Dekel, Space Security: National Capabilities and Programs, United Nations Institute for Disarmament Research (Apr. 2011); and Lubos Perek, *Space Debris Mitigation and Prevention: How to build a stronger international regime*, 2 ASTROPOLITICS 215 (2004).

[33] World Economic Forum, *supra* note 27

[34] *Supra* note 31, IV-17. *See also* Joint Chiefs of Staff, Joint Publication 3-12, *Cyberspace Operations*, US DEP'T OF DEFENSE (2013).

systems, and the like.[35] One 2014 observer noted that, this phenomenon highlights the strategic threat exposure of satellite communications:

> 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.[36]

There are additional ramifications of virtual ASAT as well, especially where commercial and economic considerations are impacted. A recent example is the November 2015 loss of communications with Israel's Amos 5 satellite, for reasons unknown publicly at the time of this writing.[37] In the days following the lapse in

[35] See *Defending the Networks: The NATO Policy on Cyberdefense*, NATO (Oct. 4, 2011), *available at http://www.nato.int/nato_static/assets/pdf/pdf_2011_08/20110819_110819-policy-cyberdefence.pdf*;Council Framework Decision 2005/222/JHA, Feb. 24, 2005 OJ L 69 (EC), p. 67; Council Directive 2008/114/EC, Dec. 8 2008 OJ L 345 (EC), p. 75.

[36] Zenko, *supra* note 31. *See also GPS Jamming: Out of Sight*, THE ECONOMIST (July 27, 2013), http://www.economist.com/news/international/21582288-satellite-positioning-data-are-vitalbut-signal-surprisingly-easy-disrupt-out.

[37] Michael Rochvarger, *Contact Lost with Israeli Communication Satellte Amos 5*, HAARETZ (Nov. 21, 2015), http://www.haaretz.com/israel-news/business/1.687543.

communications, the satellite's owner, Spacecom, registered a loss of one-third of its revenue.[38]

C. HYBRID ASAT

A combination of kinetic and physical ASAT, or hybrid ASAT, also threatens satellite communications. A hypothetical example is a satellite's communications being disrupted by the replacement of a commercial news channel's broadcast with a propaganda broadcast on the part of a rebel group, followed by a physical attack on one of the satellite's earth stations. Such an event would bear legal implications under several legal regimes, important to consider yet beyond the scope of the current analysis.[39]

D. THE NEED FOR APPROPRIATE LEGAL RESPONSES

Given both kinetic and cyber threats to satellite communications, there is a clear need for ongoing clarification of and compliance with the international legal norms that are applicable to the new challenges posed by contemporary cyber-mediated ASAT capabilities. The international community has identified this need in multiple *fora* in recent years. The following are some examples of

---

[38] Adi Ben-Israel, *Spacecom plunges after Amos 5 satellite contact lost*, GLOBES (Nov. 22, 2015), http://www.globes.co.il/en/article-spacecom-loses-contact-with-amos-5-satellite-1001082734.

[39] *See* Sascha Bachman & Hakan Gunneriusson, *Terrorism and Cyber Attacks as Hybrid Threats: Defining a Comprehensive Approach for Countering 21st Century Threats to Global Risk and Security*, 9 J. TERRORISM AND SEC. ANALYSIS 26 (2014).

states currently addressing the uncertainty of space law.

- In June 2014, an updated version of China and Russia's joint draft Treaty on the Prevention of the Placement of Weapons in Outer Space was proposed, reaffirming the importance of strict compliance with the existing multilateral agreements related to outer space activities.[40]

- In March 2014, the European Union updated its Draft International Code of Conduct for Outer Space Activities, noting the need for compliance with existing legal norms and reiterating "…their support to encouraging efforts in order to promote universal adoption, implementation, and full adherence to such instruments"[41]

- A July 2013 report by the Group of Governmental Experts on Outer Space Transparency and Confidence-Building Measures in Outer Space Activities, authorized by UNGA Resolution 65/68, identified specific measures in order to

[40] Draft Treaty on the Prevention of the Placement of Weapons in Outer Space, the Threat or Use of Force against Outer Space Objects, June 10, 2014; *See* Michael Lister & Rajeswari Rajagopalan, *The 2014 PPWT: a new draft but with the same and different problems*, THE SPACE REVIEW (Aug. 11, 2014), http://www.thespacereview.com/article/2575/1.

[41] European Union, Draft International Code of Conduct for Outer Space Activities (Mar. 31 2014), art. 3.1.

> stabilize inter-governmental uncertainty originating in space-based activities.[42]

These and other developments mark a new level of international concern with the threats to international peace and security caused by space activities. However, none of them address specifically the issue of hostile interference with satellite communications and its legal ramifications.[43] Herein we propose a normative framework for this process, and recommend that it be carried out within an appropriate multi-stakeholder administrative framework at the international level that will expand the scope of engagement of the current Committee on the Peaceful Uses of Outer Space (COPUOS).[44] Others have called for a similar administrative framework to address ASAT and other short- and long-term challenges facing space systems.[45]

---

[42] Transparency and Confidence-Building Measures in Outer Space Activities, UN OFFICE FOR DISARMAMENT AFFAIRS (Dec. 2013), http://www.un.org/disarmament/publications/studyseries/en/S S-34.pdf.

[43] The European Union Draft Code of Conduct refers in several articles to the prohibition on 'harmful interference" with space activities, although the context appears to be broader than harmful interference with satellite communications in the meaning given to this term of law by the ITU basic documents (*infra*, note 62).

[44] The work of COPOUS, established in 1959 by the UN General Assembly, is available on its website. *See* http://www.unoosa.org/oosa/en/ourwork/copuos/index.html.

[45] *See* the EU Draft Code of Conduct, *supra* note 41; Proc. of the Int'l Conf. on New Challenges in Space Law, *The Space Treaties at Crossroads: Considerations for de lege ferenda*, August 2015; *See also* Isavella Vasilogeorgi, *International Administrative Law Seedlings within the OST: Inchoate Foundations for an International Space Organisation*, Proc.

Two preliminary points should be noted before we embark on the analysis of the four regimes that constitute the normative framework. First, the convergence of the four regimes reviewed 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 increasing concern to states. How does the law presently provide responses to states, organizations and corporations that have undergone hostile disruption to their satellite communications, either by kinetic or cyber means? What are the *lex ferenda* considerations for further development of this body of law?

Secondly, the international law applicable in cyberspace, although still developing and, in particular, not yet well-supported by state practice, will at some future point directly affect state activities relating to satellites and satellite transmissions that take place in cyberspace. The merging of norms that will develop regarding satellite communications in cyberspace with the four legal regimes reviewed herein will be explored below.

III. APPLICABLE INTERNATIONAL LAW REGIMES

This section will propose a normative hierarchy of the four legal regimes reviewed, in order to proceed with an examination of how a cooperative framework among states and relevant international organizations might be developed to

---

of the Int'l Conf. on New Challenges in Space L.. *available at* http://www.nb.org/files/SpaceLaw_Programma.pdf.

address cyber-mediated ASAT the aim of which is the disruption of satellite communications. We will move from the regime most general in its application to the most specific in its application. The first reviewed is the collective security regime set out in the UN Charter. Following is the Universal Declaration of Human Rights' Article 19 transborder freedom of information; then international telecommunications law; and finally space law, which applies specifically to space objects, including satellites.[46] We note at the outset of this section that each of these regimes is a complex one in and of itself, deserving of detailed analysis; the discussion below touches on some of their highlights.

A. COLLECTIVE SECURITY UNDER THE UN CHARTER

Hostile disruption of satellite communications on the part of state actors, as well as disruption due to error, negligence and other non-hostile motivations, raises questions under international law around the applicability to such acts of collective security regime within the UN Charter. In particular, it raises the question of whether hostile virtual disruptions constitute a violation of the Charter's Article 2(4), which

[46] The analysis below follows that by the present author in *Cybersecurity Threats to Satellite Communications: Towards a Typology of State Actor Responses*, Proc. of the Int'l Astronautical Federation's 66th Int'l Astronautical Cong., (2015), *supra* note 7.

prohibits the use of force or its threat among states, as follows:[47]

> All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.

The Article 2(4) prohibition on the use of force is binding on all states. Yet the question of a 2(4) violation is particularly challenging when the disruptions are virtual or hybrid, rather than strictly physical.[48]

Some international law initiatives, most prominently the 2014 Tallinn Manual, engage with the issue of whether state activities in cyber space, if sufficiently damaging, may be held by victim states to constitute an illegal use of force in the meaning of Article 2(4) of the UN Charter.[49] The international law is still evolving regarding the parameters of the applicability of this provision in cyberspace, as well

---

[47] U.N. Charter art. 2(4), *available at* https://treaties.un.org/doc/publication/ctc/uncharter.pdf.

[48] Physical attacks on satellites are sufficiently dealt with under the space law conventions. *See, e.g.*, art. III of the OST, *infra* note 73, and Michel Bourbonniere, *Law of Armed Conflict (LOAC) and the Neutralisation of Satellites, or Ius in Bello Satellitis*, 9 J. OF CONFLICT AND SEC. L. 43 (2004).

[49] 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, *supra* note 12; Developments in the Field of Information and Telecommunications in the Context of International Security, UN OFFICE FOR DISARMAMENT AFFAIRS (Dec. 2011), http://www.un.org/disarmament/HomePage/ODAPublications/DisarmamentStudySeries/PDF/DSS_33.pdf.

as the permitted parameters of self-defense against "an armed attack" under the Charter's Article 51.[50] This article ensures a state's inherent right to self-defense "if an armed attack occurs"[51] One example of such an armed attack might be the intentional disruption of satellite transmissions that provide air traffic control towers with data on airplane traffic and the planes themselves with navigation signals, causing aircraft accidents and consequent loss of human life.

The as-yet-unresolved issue of whether a virtual attack on a satellite system is in fact an armed attack under the Charter is a compelling one for an increasing number of states. The degree of damage required in order for a disruption to constitute a prohibited use of force is still an open question – one avenue for its resolution is the Tallin Manual's dual test of requiring scope and effect equivalent to that of a physical attack.[52]

---

[50] 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. *See* Michael Schmitt and Liis Vihul, *The Emergence of Legal Norms for Cyber Conflict*, in BINARY BULLETS: THE ETHICS OF CYBERWARFARE (Fritz Allhoff et. al. eds., 2014)

[51] The text of the article, in its entirety is: "Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security." UN Charter, *supra* note 47).

[52] Rule 11, Tallinn Manual, *supra* note 12, p. 45.

Increasingly, state and non-state actors are interested in knowing under what circumstances disruption of a satellite transmission constitutes an attack that may justify self-defense under Article 51, or other legitimate self-help under international law; and what the parameters of legitimate responses to such an act may be.[53] This issue is especially cogent given the present role of satellite communications as key elements of governmental, financial, commercial and military systems. Critical infrastructure installations that are dependent upon satellite communications are especially at risk to ASAT in this context.

B. TRANSBORDER FREEDOM OF INFORMATION FLOW

The second legal regime relevant to the protection of satellite transmissions from harmful disruption is that of the freedom of transborder information flow. This regime deals both with technical disruptions and with content-related aspects of communications.

---

[53] See for instance, Michael Schmitt, *Rewired Warfare: Rethinking the Law of Cyber Attack,* 96 INT'L REV. OF THE RED CROSS (2014); Thomas Wingfield, *Legal Aspects of Offensive Information Operations in Space*, 9 USAF Academy J. of L. Stud., (1998-99;); Bourbonniere, *supra* note 48; Kurt Schendzielos, *Electronic Combat in Space: Examining the Legality of Fielding a Space-Based Disruptive Electromagnetic Jamming System* (June 15, 2007) (Master's Thesis). 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), http://www.economist.com/node/16478792; *NATO 2020: Assured Security; Dynamic Engagement*, NATO (May 17, 2010), http://www.nato.int/cps/en/natolive/official_texts_63654.htm.

Freedom of communication over national borders is recognized by both treaty law and customary law. It is formulated in Article 19 of the 1949 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. [54]

This formulation is broadly-drafted, and is intentionally technology-neutral: it applies to satellite communications just as it applies to printed newspapers. The freedoms set out in Article 19 are supported by customary international law, rooted in 19th century Western European concepts of democracy and freedom of expression.[55] Interestingly, an early effort to restrict such transborder freedom of information exchange was promoted in the 1936 International Convention Concerning the Use of Broadcasting in the Cause of Peace.[56] This treaty, by prohibiting among its signatories the use of hostile propaganda and incitement to war, attempted to respond to public

---

[54] G.A. 217 A (III) (Dec. 10, 1948). 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".

[55] *See* Peter Malancuk, *Information and Communication, Freedom of, in* ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW 148 (Rudolf Bernhardt et al. eds.,1986).

[56] International Convention concerning the Use of Broadcasting in the Cause of Peace, Sept. 23, 1936, p. 301.

incitement to war *via* the new technology of 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".[57]

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 or otherwise block propaganda broadcasts from hostile states was debated by international lawyers.[58] This legal debate was further carried over into the 1970s, in the context of direct broadcast satellite (DBS) transmissions and the resulting "free flow versus prior consent" argument.[59] Still, the scope of Article 19's freedom of information transfer remains unclear. International law recognizes limitations on the freedom of transborder communication, including satellite transmissions, largely on the basis of a state's sovereign right to control the communications that occur within its own territory, or that emanate from it. This freedom may be curtailed, for instance, by domestic law provisions,

---

[57] *Id.*

[58] *See* John Whitton, *Cold War Propaganda*, 45 AM. J. INT'L L. 151 (1951); and Jamie Metzl, *Rwandan Genocide and the International Law of Radio Jamming*, 91 AM. J. INT'L L. 628 (1997), at 636-645; Deborah Housen-Couriel, *International Telecommunications Law and International Cyber Law* (Hebrew), *in* INTERNATIONAL LAW (Robbie Sabel ed., 3rd ed.) (forthcoming).

[59] James Savage and Mark Zacher, *Free flow vs. prior consent: The jurisdictional battle over international telecommunications*, 42 INT'L J. 342 (1987).

such as those addressing national security issues,[60] by the Security Council acting under Article 41, and possibly by *jus cogens* considerations (*i.e.*, to prevent incitement to genocide).[61]

C. INTERNATIONAL TELECOMMUNICATIONS LAW

The field of international telecommunications law, or ITL, has been developed largely under the aegis of the leading inter-governmental organization in the field, the International Telecommunications Union (ITU). The organization serves also as the UN specialized agency charged with the global regulation of telecommunications. The ITU Constitution has consistently defined the term "telecommunication" broadly, encompassing satellite (and other) communications utilizing both wireless and wired infrastructures; on the earth, in the atmosphere, and in outer space.[62]

At the technical level, the ITU's Radiocommunications Sector assigns orbital slots and coordinates to satellites, at the request of the relevant states, and maintains the Master

---

[60] On the balancing of these considerations, *see*, *e.g.*, *Global Principles on National Security and the Right to Information ("The Tshwane Principles")*, OPEN SOCIETY JUSTICE INITIATIVE (June 12, 2013), *available at* https://www.opensocietyfoundations.org/sites/default/files/global-principles-national-security-10232013.pdf.

[61] *See* Metzl, *supra* note 58.

[62] ITU CONSTITUTION, Annex 1012, *available at* http://www.itu.int/en/history/Pages/ConstitutionAndConvention.aspx.

International Frequency Register (MIFR)[63] relating to satellite registration according to country, uplink and downlink frequency assignments, orbital location, and satellite expiry date.[64] More substantively, Article 33 of the ITU Constitution prescribes the non-discriminatory use of 'the international service of public correspondence", including relevant satellite communications, as follows:

> 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. [65]

Articles 34 and 35, entitled respectively "Stoppage of Telecommunications" and "Suspension of Services", balance out this right by permitting states to suspend ingoing and outgoing telecommunications, including satellite communications, with respect their own territory, on the condition that they publicly notify the stoppage or suspension, as stipulated.[66]

Examples of two additional ITU provisions that are particularly relevant to satellite

---

[63] *See Space Plan Assignments Recorded in the Master Register*, ITU (last modified Aug. 12, 2015), *available at* http://www.itu.int/en/ITU-R/space/plans/Pages/MIFR.aspx.

[64] The ITU provides extensive information on the MIFR and the regulatory processes applicable to satellites. *See* the ITU website (www.itu.int); Yvon Henri, *Satellite International Regulatory Framework: Added Value or Hindrance to Development*, ITU-R, 3-4 (Feb. 2010).

[65] ITU Constitution, *supra* note 62, art. 33.

[66] *Id.*

transmissions are Articles 44 and 45. Article 44 provides that the global electro-magnetic spectrum 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…."[67] This provision is directly applicable to satellite systems and transmissions, providing an internationally-agreed characterization of these resources that has legal ramifications on the provision of uplinks and downlinks, for instance.

Finally, Article 45 of the Constitution prohibits states from disrupting all transborder wireless communications, including satellite transmissions, from "harmful interference". This term is defined in detail by Article 15 of the 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."[68] It is also worth noting that emergency communications are given special protection in the Regulations, and receive "absolute priority"[69] over other types of telecommunications. The ITU Constitution's exemption of military installations, including military satellite installations, from the two latter normative

[67] *Id.*

[68] *ITU Radio Regulations*, ITU (2012), *available at* http://www.itu.int/en/ITU-R/terrestrial/tpr/Documents/Article15-RR12.pdf.

[69] "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." *Id.*

provisions does complicate the application of the ITU legal regime across all satellite system infrastructures.[70] This is due to the overwhelmingly dual-use nature of contemporary satellite systems. 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.[71]

To summarize, ITL, as expressed in the constitutional provisions of the ITU, provides a relatively clear and widely-accepted normative and regulatory position that supports uninterrupted satellite communications when these cross state borders. Moreover, the ITU norms specifically prohibit harmful interference with satellite transmissions. They also require states to operate with transparency regarding any interruptions to the transborder satellite communications of other states. These ITL provisions are rooted in a robust regime that has developed over the course of the evolution of wireless and wired communications since the 19th century and into the age of global satellite communications.[72]

D. SPACE LAW

---

[70] *Id.*, at art. 48.

[71] J. Del Rosario and C. Rousseau, *An Analysis of Hosted Payloads and Dual-use Satellites as Middle Ground between Commercial Outsourcing and Internal Asset Deployment*, INTERNATIONAL SPACE UNIVERSITY, http://www2.isunet.edu/index2.php?option=com_docman&task=doc_view&gid=762&Itemid=26.

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

The final regime for analysis is space law. It is the newest of the four reviewed here, having developed in the wake of the genesis of space exploration in the 1950s. There are five treaties specifically drafted under the aegis of the United Nations and applying to several aspects of human endeavor in space, with the most comprehensive being the 1967 Outer Space Treaty (OST).[73] In addition to treaty law, some experts argue that customary law has formed as well, drawing on the relatively small community of space-faring states.[74]

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 shall be free for exploration and use by all states, in accordance with international law. Article III encompasses the collective security regime set out in the UN Charter and discussed above.[75]

---

[73] 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 Status of International Agreements relating to activities in outer space as at 1 January 2015*, UN OFFICE FOR OUTER SPACE AFFAIRS (Apr. 8, 2015). For review and analysis of the law of space as it relates to satellites, *see* Nandasiri Jasentuliyana, *A Survey of Space Law as Developed by the United Nations*, in PERSPECTIVES ON INTERNATIONAL LAW, (Nandasiri Jasentuliyana ed., 1995).

[74] *See* Michael Listner, *Customary international law: A troublesome question for the Code of Conduct?*, THE SPACE REVIEW (Apr. 28, 2014), http://www.thespacereview.com/article/2500/1.

[75] The Article states: "Outer space, including the moon and other celestial bodies, shall be free for exploration and use by

States may not claim sovereignty over locations in space such as moons or planets,[76] yet they retain sovereignty and control over satellites and other space objects that they either own or have launched into space. States also retain liability for any damage caused by such objects.[77] Article VII is the operative provision.[78] Thus, space law imposes upon states the responsibility for actions carried out by means of satellites under their jurisdiction and control. These actions include physical damage

---

all States without discrimination of any kind, on a basis of equality and in accordance with international law." (emphasis added). Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies (1967); G.A. Res. 2222 (XXI), 1966. As of October 2011, 100 countries (including Israel) are parties, while another 26 have signed but have not completed ratification.

[76] "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". *Id.*, at art. II.

[77] Art. 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. *Id.*, at art. VI

[78] The Article states "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." (emphasis added). *Id.*, at art. VII.

caused by the creation of space debris that inflicts physical harm to other states' satellites.[79]

The comprehensive legal regime establishing responsibility and stipulating damages is set out in the Liability Convention, elaborating OST Article VII in establishing absolute liability "for damage caused by its space object on the surface of the earth or to aircraft flight."[80] This liability requires payment of compensation when appropriate criteria have been met. In other non-terrestrial areas such as outer space, state liability must be established under 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."[81]

---

[79] *See, e.g.*, Robert Merges and Glenn Reynolds, *Rules of the Road for Space?: Satellite Collisions and the Current Inadequacy of Space Law*, 40 ENVTL. L. REP. 10009 (2010), *available at* https://www.law.berkeley.edu/files/article-2011-10-40.10009-1.pdf.

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

[81] Liability Convention, *supra* note 80, art. I. *See* Julian Hermida, *International Space Law*, *in* LEGAL BASIS FOR A NATIONAL SPACE LEGISLATION (2004); Michael Listner, *Revisiting the Liability Convention: reflections on ROSAT, orbital space debris, and the future of space law*, THE SPACE REVIEW (Oct. 17, 2011), http://www.thespacereview.com/article/1948/1.

This was one of the salient provisions regarding the legal controversy around the 2009 Russian Kosmos satellite collision with an iridium communications satellite, referred to above. The applicability of the Liability Convention to satellite transmissions that have been disrupted through solely virtual means, in cyberspace remains an open issue. We propose here that a reasonable interpretation of Article VII does include damage caused by a hostile disruption to satellite transmissions. 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. We believe this is not an unreasonable extension of the scope and intention of the Convention, especially given the high commercial and financial value of many satellite transmissions.

The WIPO Convention to satellite transmissions, which are viewed therein as assets capable of bearing proprietary rights also provides a precedent.[82] In support of this approach, it should also be noted that many commercial satellite operators and satellite consortia, such as International Maritime Satellite Organization (IMSO), are bound to provisions within their particular conventional regimes that impose liability and require compensation when client transmissions are interrupted, distorted or otherwise damaged.[83]

---

[82] *See Technological and Legal Developments in Intellectual Property*, *in* WIPO INTELLECTUAL PROPERTY HANDBOOK: POLICY, LAW AND USE 451-453 (2004).

[83] IMSO Convention, G.A. Res. 1721 (XVI), 2008; LRIT Agreement, IMSO, *available at* www.imso.org/LRIT.

Thus, the application of space law to the disruption of satellite transmissions may be summarized as follows. Its determinative point of departure is general international law, including the UN Charter and the regime of collective security reviewed above. Although the treaty regime stipulates that states may not claim sovereignty over particular territories in outer space, including the moon and other celestial bodies, satellites are different. They in fact remain under both the sovereignty and the responsibility of the launching state or states. These legal principles have been established in the OST, which also provides (together with the Liability Convention) for the liability of states for damage caused by satellites from the launch stage and thereafter, throughout the satellite's life span.

Moreover, the definition of "damage", crucial to the application of the Liability Convention, is broad, and 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, and the applicable commercial satellite agreement. In this author's view, satellite transmissions are in fact subject to the Liability Convention and protected as "property" by its provisions. Nonetheless, state practice regarding the issue is currently insufficient, as it is regarding the enforcement of the Liability Convention with respect to physical damage to satellites.[84]

---

[84] *See Settlement of Claim between Canada and the Union of Soviet Socialist Republics for Damage Caused by "Cosmos 954*, Ru.-Ca., April 2, 1981, *available at*

V. CONCLUSIONS

International law plays a central role in articulating the constraints applicable to state activities relating to satellite communications. This function encompasses the elucidation of norms and of enforcement mechanisms stemming from the four legal regimes reviewed above, relating to the imposition of effective sanctions on states that engage in hostile interruption of communications. In addition, it is increasingly important to consider the range of possibilities for state responses to hostile disruptions to satellite communications in light of the new issues arising from the application of international law to state activities in cyberspace. The regimes addressing collective security, freedom of expression, international telecommunications law and space law are at present relatively well-understood as independent regimes. Their convergence in a nexus is more challenging. Nonetheless, a comprehensive understanding of interaction of these regimes around issues of state liability for hostile disruption of satellite communications, especially cyber-mediated disruption, has not yet matured.

Given the strategic and tactical threats posed by cyber-mediated ASAT at present, a, multi-stakeholder review of the measures available under international law in response to hostile acts directed at satellites and satellite transmissions should be

---

http://www.spacelaw.olemiss.edu/library/space/International_Agreements/Bilateral/1981%20Canada-%20USSR%20Cosmos%20954.pdf; Eilene Galloway, *Nuclear Powered Satellites: The U.S.S.R. Kosmos 954 and the Canadian Claim*, 12 AKRON L. REV. 401 (1979).

undertaken with some urgency. Due consideration should be given to the rapid development of ASAT capabilities by a number of states, and perhaps non-state actors, as well. The appropriate multi-stakeholder administrative framework at the international level may well begin by expanding the existing scope of the Committee on the Peaceful Uses of Outer Space (COPUOS). *Lex ferenda* considerations, in this author's view, should include both further clarification of the operative nexus of the four regimes reviewed above, and the incorporation into that nexus of developing norms of international law in cyberspace applicable to satellites and satellite communications.