中国空间法年刊

————2017————

Chinese Yearbook of Space Law

李寿平主编

Editor –in-Chief：Li Shouping

世界知识出版社

Words Can Never Hurt Me: Cyber Technologies, Satellite Information Flows, and Liability for Space Activities[①]

P.J. Blount [*]

In 2014, the United States Supreme Court decided the case of *Riley v. California*.[②] In this case, the applicant had been arrested by law enforcement. Subject to that arrest the police searched the person on the applicant and found his cell phone. The officers then opened the cell phone and looked at the data contained therein for more evidence, and in this case they found evidence linking the applicant to other crimes. The court was faced with determining whether in a search incident to an arrest law enforcement needed a search warrant under the US constitution to search the arrestees cell phone. In general, the police have the ability to search an individual that has been arrested without a warrant. Previously, the Court upheld a police searches that opened a package of cigarettes found in the arrestee's pocket to reveal drugs inside.[③] The problem in Riley, though, was different, and it was different because it involved data. In a sense the court had to make a determination of what was actually in the individuals pocket. In the case of a cigarette package containing drugs, it is easy to assess that both the package and the illegal drugs are *in* the individual's pocket. The *Riley* court, on the other hand, had to address whether the data on the phone was in the individuals pocket. This is difficult because "[c]ell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person. The term "cell phone" is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone."[④] The court had to distinguish between the physical object in the arrestee's pocket and the immense access to data that was contained on that object.[⑤]

While the Riley is substantively distant from the cope of this article, the legal line drawing that the US Supreme Court engaged in is becoming emblematic of the law and policy issues that are arising in a digitized and networked world. The central problem is that it is becoming increasingly unclear where to separate data flows from the physical objects those data flows move across from the individuals accessing those data flows. The Riley Court acknowledges this problem when it states that cell phones and their associated data flows are a "pervasive and insistent part of daily [such] life that the proverbial visitor from Mars might conclude they were an important feature of human

---

① This paper is based on a presentation given at the Space Security and Long-term Sustainability of Outer Space Activities Conference held at the Chinese University for Political Science and Law on May 25, 2014.

* B.A./A.B.J., University of Georgia; J.D., University of Mississippi School of Law; LL.M., King's College London; M.S./Ph.D., Rutgers University. Blount serves as an Adjunct Professor in the L.L.M. in Air and Space Law at the University of Mississippi School of Law. He is also the editor-in-chief of the Journal of Space Law and a board member of the International Institute of Space Law.

② Riley v. California, 134 S. Ct. 2473 (2014).

③ United States v. Robinson, 414 US 218 (1973)

④ Riley at 2489.

⑤ The Court did indeed rule that the search of the phone required a warrant under the 4th Amendment of the U.S. Constitution. Riley at 2495.

anatomy."[①] This is because one of the signature features of the ongoing Information Age is the convergence of technology.[②] Technologies that were once discreet are now interlinked and indiscrete by the increasingly rapid flow of bits and bytes rendering the underlying technologies indistinguishable from each other. The modern smart phone is the quintessential example. While we call them "phones" because they can make and receive voice calls, smart phones "could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers."[③] Digitization and networkification flatten multiple technologies into single devices, and space technology has not been immune to the convergent effects of cyber technologies. Indeed, space capabilities have fueled this convergence by serving as a key link in connecting data and as key source for data collection. For instance, everyday electronic devices (such as cell phones) can take data derived from satellites (such as geospatial information) and transmit it to a multitude of places simultaneously through the global telecommunications networks which often routes via telecommunications satellites. The effects of these changes on society, whether negative or positive, are impossible not to take note of as the individual is increasingly merged with and implicated in the technological devices.[④] As technology converges, though, legal regimes warp and collide along geographical and subject matter jurisdictional lines.[⑤]

This paper will investigate how technological hybridity can warp legal doctrines by causing interpretive conundrums, and it will focus specifically on the issue of liability for cyber activities that route through the space segment. First, the paper will address the dynamic nature of the interactions between law and technology, and illustrate how cyber technologies are causing disruptions in this dynamic. Building on the conceptual background of the first section, Section II will examine the law and technology dynamic in the specific context of the Liability Convention's application to the case of space harms caused through the use of cyberspace. Finally, the paper will discuss analytic and interpretive strategies that may be helpful in framing these issues and determining the most just result. The adopted approach with be theoretical, and does not seek to identify specific answers, but instead to analyze the salient features for approaching mixed legal spaces that result from converging technologies.

I. Law and Technology

Law have historically been in perpetual interaction with each other.[⑥] The nature

---

① Riley at 2484.

② Damian Tambini, Danilo Leonardi, and Christopher T. Marsden, *Codifying Cyberspace: Communications Self-Regulation in the Age of Internet Convergence*: Routledge, 2008, p.3-4.

③ Riley at 2489.

④ This is not to say that humans have become cyborgs, but instead that in the developed world humans have integrated machines (for lack of a better general term) into their everyday life in almost all facets of life. The extent and meaning of such integration is hotly contested. For a taste of the sociological debate see *Cyborgology*, http://thesocietypages.org/cyborgology/ 登录时间：2014 年 9 月 22 日。

⑤ Kulesza, Joanna. *International Internet Law*. Translated by Magdalena Arent and Wojciech Wotoszyk: Routledge, 2013, chap. 1.

⑥ For example, Hammurabi's code features extensive regulation of agriculture technology. *Hammurabi's Code of Laws*, trans. L.W. King, http://eawc.evansville.edu/anthology/hammurabi.htm 登录时间：2014 年 9 月 22 日.

of these interactions is a non-hierarchical relationship. In other words, law drives technological change, *and* technology drives legal change. There are two key aspects to this law-technology dynamic that must be understood. First s the is the dynamic in terms of the legal spaces occupied, and second, the dynamic in terms of relative effects when either law or technology changes not in tandem with the other. This second aspect is most often observed when technological change that strains the existing legal framework.

The first aspect of the law-technology dynamic is primarily concerned with how the law creates legal spaces around specific technologies.[①] There are two primary ways in which technology is regulated. First, there are laws that focus on regulating the conduct of individuals in their use of technology. So for instance, international humanitarian law affects technology by placing limitations on how a combatant may use technology. Legal regimes of this type create law governing certain activities that intersect with technology, and the legal space that is created surrounds the human actor as opposed to the technological components.[②] Space law serves as an excellent example of this as its application is triggered when the technology of a 'space object' is used.[③] In a similar fashion, non-proliferation law governs nuclear technologies based on the existence of the technology itself. With this type of regulation, the legal space is approximately congruent with the technological space. While, regulation of technology is usually a mixture of these types of regulations, the second type raises specific concerns in that it compartmentalizes the application of the law to the space in which the technology exists. This means that at the edges of the legal space, another legal regime is meant to begin, and the nature of the law is that some legal spaces are left with gray edges,[④] which often intersect and create complicated governance questions. An example of these gray edges can is readily seen in the undefined area between aviation law and space law created by the lack of spatial delimitation. These legal spaces are congruent with technologically created space thereby minimizing the size of the liminal areas where both or neither law may apply.

Second, the law-technology dynamic must be appreciated in terms of how law and technology interact. As stated earlier, these two concepts are intermingled. Law is most often driven by a need to adapt to emerging technologies. As a result, law is often reactionary to technological development. An analog to this premise is that law rarely anticipates new technologies. The legal vacuum that met *Sputnik I* after its 1957 launch is

---

① Legal space in this sense is different from a jurisdiction, which would involve the ability of a lawmaker to take action, in that it implies a subject realm the edges of which are reasonably well fixed.

② For example, "expanding bullets" can be legal at the domestic level for law enforcement and recreational purposes, but are prohibited in armed conflict. *See generally*, Yoram Dinstein, *The Conduct of Hostilities Under the Law of International Armed Conflict*. Cambridge University Press, 2004, p. 64.

③ On the nexus between space law and 'space objects' see Christopher M. Hearsey, "The Evolution of Outer Space Law: An Economic Analysis of Rule Formation" (University of North Dakota, 2015) at Chaps. IV & V.

④ As in cases where there is no "bright line rule."

illustrative, especially so since this flight arguably settled the legal question of satellite overflight.[①] In this reactionary state, law can change the way that technology develops in a variety of ways, but namely by opening or closing paths of innovation. An example of this can be found in the United States Human Space Flight Requirements, which sought to open pathways to innovation by not using the law to restrict the available technology.[②] An opposing example would be the "clipper chip" debate in which the U.S. government attempted to set limits on innovation paths by attempting to restrict technological standards.[③]

These two types of interactions can be observed in the development of traditional telecommunications law, which is of particular relevance to the topic at hand, because telecommunications law forms the roots of cyberspace law and governance. Telecommunications law has traditionally been compartmentalized along technological borders. In other words, laws governing radio are different from laws governing telephones which are different from laws governing cable service and so on.[④] This is because each technology's underlying policies were customized to the particular challenges presented by each discrete manifestation of telecommunication technology. For example, while satellite telecommunications are governed to maximize the use of scarce orbit-spectrum resources,[⑤] telephone services are governed to maximize universal access.[⑥]

This is important, because the technology of cyberspace, creates a major shift in the law-technology dynamic by erasing these technological borders and increasing the gray areas in which legacy rules of law operate.[⑦] As a result, the applicable legal doctrines become warped out of their once clear compartmentalizations. The problem cyberspace creates, from a governance perspective, is that it is unclear where cyberspace begins and ends in cultural, technological, and legal senses. This quite literally creates jurisdictional disputes, as well as a lack of clarity in choice of law issues.[⑧] Cyberspace is a

---

① Walter A. McDougall, Heavens and the Earth. New York: Basic Books, 1985, p. 134.

② See generally Hughes, Timothy Robert, and Esta Rosenberg. "Space Travel Law (and Politics): The Evolution of the Commercial Space Launch Amendments Act of 2004." J. Space L. 31, 2005, p.1 and Knutson, Tracey. "What Is Informed Consent for Space-Flight Participants in the Soon-to-Launch Space Tourism Industry." J. Space L. 33, 2007, p.105.

③ Lessig, Lawrence. Code 2.0. Basic Books, 2006, p. 66-67.

④ See generally, Krattenmaker, Thomas G. Telecommunications Law and Policy. 2nd ed. Durham, NC: Carolina Academic Press, 199 and Kennedy, Charles H., and M. Veronica Pastor. An Introduction to International Telecommunications Law. Boston: Artech House, 1996.

⑤ Roberts, Lawrence D. "Lost Connection: Geostationary Satellite Networks and the International Telecommunication Union, A." Berk. Tech. LJ 15, 2000, p.1095 and Copiz, Adrian. "Scarcity in Space: The International Regulation of Satellites." CommLaw Conspectus 10, 2001, p.207.

⑥ Krattenmaker, Telecommunications Law and Policy, p. 463-479.

⑦ Cyberspace is made possible by a communications protocol (TCP/IP) that is indifferent to the telecommunications technology that is transmitting it. Post, In Search of Jefferson's Moose, pp.88-89 and Lessig, Code 2.0, p.143-45.

⑧ The classic examples being the France v. Yahoo! case surrounding the sale Nazi paraphernalia online and the Germany v. Compuserve case involving the distribution of pornography online.

cultural phenomenon that has developed around the technology of the Internet, which allows for the networking of electronic devices via software standards and protocols.[①] The extent of the network is virtually limitless.[②] In light of technologies that enable the so called "Internet of Things," cyberspace is a vast technological phenomenon that intersects with the average individual - in the developed world and increasingly in the developing world - multiple times each day.[③] This also means that as more devices interconnect and depend on the network, the more cyberspace as a technology will infiltrate a variety of other legal spaces. This infiltration warps the interaction of law with technology. So, for instance, one of the central themes in the United States National Security Agency documents revealed by Edward Snowden was the tension between the way the law governing previous technologies in the context of national security had been vastly changed by the new capabilities presented by Cyberspace.[④] This is not a phenomena unique to national security and has been observed in intellectual property law and human rights law among others.[⑤] Cyberspace in each of these cases challenges the underlying assumptions about how a discrete technology works by converging it with other technologies.

This creates a difficult problem for governance. The regulated are often faced with a lack of clarity in the applicable law and a clash of underlying regulatory values as the legal and technological spaces around them are merged and warped. Often these are characterized by negative outcomes as determined by the underlying values of at least one of the underlying regulatory regimes. One of the reasons for this is that cyberspace is

---

See Lessig, Code 2.0, at p.34, 294-295; Kulesza, International Internet Law.at p.106-8; and Post, David G. In Search of Jefferson's Moose: Notes on the State of Cyberspace. Oxford; New York: Oxford University Press, 2012, p. 164-71.

For the classic article on this idea see David R. Johnson and David Post, "Law and Borders: The Rise of Law in Cyberspace," Stanford Law Review 48, No. 5, 1996, pp.1367–1402.

① For cyberspace as a cultural space see generally, Lessig, Lawrence. *Free Culture : The Nature and Future of Creativity*. New York: New York : Penguin Books., 2004; Lessig, *Code 2.0*, at chap. 2; and Kellner, Douglas. "Intellectuals, the New Public Sphere, and Technopolitics." in *The Politics of Cyberspace*, edited by Chris Toulouse and Timothy W. Luke, New York: Routledge, 1998, pp.147–86.

② A dramatic example of the limits of the network is the Stuxnet virus which jumped a an "air gap" in order to attack an Iranian nuclear facility. Bruce Schneier, "Air Gaps," *Schneier on Security*,, https://www.schneier.com/blog/archives/2013/10/air_gaps.html. 登录时间：2013 年 10 月 11 日。

③ *See* Stefan Ferber, "How the Internet of Things Changes Everything," *Harvard Business Review*,, http://blogs.hbr.org/2013/05/how-the-internet-of-things-cha/.登录时间：2013 年 5 月 7 日。 On the spread of the Internet of Things into space *see* P. J. Blount, "Satellites Are Just Things on the Internet of Things," *Air and Space Law* 42, No. 3, May 1, 2017, pp.273–93.

④ This can be best seen in the legal justifications for warrantless surveillance that were based on legal rules developed for telephone technologies. *See for example*, United States Department of Justice. "Memorandum for the Attorney General: Proposed Amendment to the Department of Defense Procedures to Permit the National Security Agency to Conduct Analysis of Communications Metedata Associated with Persons in the United States [Snowden Leak June 27, 2013]," November 20, 2007.

⑤ *See for example* Lessig, *Free Culture* and OSCE, *Freedom of Expression on the Internet* ,2011.

a social/cultural/societal space as well as a technological space. Technologically speaking, cyberspace is a structure built out of physical components linked on a physical network that sits in the physical territory of nation-states, but those components are just one of the elements of cyberspace. The other element is the widespread societal adoption of this technology as the predominant way to communicate and pursue cultural and economic activities. Cyberspace raises unique issues due to its strong ties to concepts such as Habermas' "public sphere."[①] Arguably, regulation of the technology that creates this space has effects on the discursive processes that underpin society at large, thus great care should be taken when regulation is applied.

II. The Liability Convention

Space is not immune to the encroachment of cyber activities into its domain. In fact, the space segment is a key link in the cyber domain, is reliant on IP based technologies, and is vulnerable to cyberattacks.[②] Satellites are transfer points for bits and bytes of data, and clever hackers can use them for their own uses.[③] Thus far hackers have been using the satellites for just that: to transfer data over the satellite's network. The capability certainly raises security concerns, as it clearly displays the vulnerability of a satellite's operating system to interference by third parties and raises the alert as to whether these parties could take control of satellites and use them for more sinister purposes.

Cyberattacks on satellites have been, in the literature, predominantly focused on the context of the law of the use of force and the law of armed conflict.[④] There is the

---

① *For example* Roper, Juliet. "New Zealand Political Parties Online: The World Wide Web as a Tool for Democratization or for Political Marketing?" in *The Politics of Cyberspace*, edited by Chris Toulouse and Timothy W. Luke,, New York: Routledge, 1998,p.69–83,and Kellner, "Intellectuals, the New Public Sphere, and Technopolitics."

② *See generally* P. J. Blount, "Satellites Are Just Things on the Internet of Things," *Air and Space Law* 42, No. 3, May 1, 2017, pp.273–93.

③ For examples see Doctorow, Cory. "Brazil Cracks down on Sat-Hackers Who Bounce Ham Signals off US Military Satellites." *Boing Boing*,http://boingboing.net/2009/04/19/brazil-cracks-down-o.html,登录时间：2009 年 4 月 19 日；"How to revive a satellite," *The Economist,* http://www.economist.com/blogs/babbage/2014/05/technoarchaeology, 登录时间：2014 年 5 月 30; James Middleton, "Tamil Tigers Hack Satellite," *The Telecoms.com,* http://www.telecoms.com/6151/tamil-tigers-hack-satellite/,登录时间：2007 年 5 月 13 日; and Mejia-Kaiser, Martha. "Space Law and Unauthorised Cyber Activities." In *Peacetime Regime for State Activities in Cyberspace*, edited by Katharina Ziolkowski, Tallin, Estonia: NATO CCD DOE, 2013, p.349–72.

④ Rendleman, James D., and Robert Ryals. "Cyber Operations to Defend Space Systems?" In *AIAA SPACE 2013 Conference and Exposition*. American Institute of Aeronautics and Astronautics, 2013. http://arc.aiaa.org/doi/abs/10.2514/6.2013-5401; Wingfield, Thomas C. "Legal Aspects of Offensive Information Operations in Space." *USAF Acad. J. Legal*9, 1998, p.121. http://heinonlinebackup.com/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/usafa9&section=11; and Petras, Christopher M. "Use of Force in Response to Cyber-Attack on Commercial Space Systems-Reexamining Self-Defense in Outer Space in Light of the Convergence of US Military and

possibility, though, that these attacks could occur outside of the context of state military action, which would position such attacks outside of the legal space triggered by an armed conflict. In such a case, it is likely international rules of responsibility and liability would come into play. Space activities and technologies are subject to the *lex specialis* of international space law, which is substantially congruent with the use space technology. Applicability of the Liability Convention and Article VI of the Outer Space Treaty are both triggered when there is a wrongful act resulting from human space activities. Cyberattacks cause strain on the terms of these legal principles by muddying the technological waters.

To assist in understanding how cyber technologies cause this strain, assume three different types of cyberattacks:

- Scenario 1 - The cyber attacker uses the satellite to transfer data to a third party that then causes damage not directly related to the satellite technology. For example the attacker uses code to shut down a power grid. In this scenario the satellite only functions as a transfer point.
- Scenario 2 - The attacker uses the satellite to transfer data to the surface of the Earth and causes damage via a direct link with the satellite. For instance, the hacking of a navigation satellite to misroute planes in flight thereby causing plane crashes. In this instance, the satellite acts as a transfer point, and the damage is directly related to that satellite's data.
- Scenario 3: The attacker uses the satellite to cause damage to another satellite. In this scenario the attacker uses the hacked satellite to cause damage to another satellite in orbit.

For each of these scenarios a few assumptions will be made to simplify the analysis. First, we will assume that these attacks are clearly the work of third parties and not the action of a state engaging in an act of armed conflict.[①] Second, we will assume that these acts are attributable to a specific party.[②] Third, each of these scenarios will treat the cyberattack as a one-time event, though in reality this is a fiction since a successful cyberattack usually requires long periods of sustained activity. Finally, it should be noted that these scenarios represent points on a spectrum of varying activities and only serve to help explicate the problem rather than serving as firm categorical typologies.[③]

The critical question, for responsibility and liability purposes, raised by a cyberattack

---

Commercial Space Activities, The." *J. Air L. & Com.* 67, 2002, pp. 1213.

① Of course, this is never that clear. For example, the U.S. Indicted Chinese PLA officers for economic espionage. U.S. v. Wang et al. - Indictment, crim. no. W.D. Penn,2014, p.14-118.

② Which is not always the case, McDermott, Rose. "Decision Making Under Uncertainty." In *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, by Committee on Deterring Cyberattacks: Informing Strategies and Developing Options; National Research Council, 227–41. Washington, D.C.: National Academies Press, 2010. http://www.nap.edu/openbook.php?record_id=12997&page=273 and Clark, David D., and Susan Landau. "Untangling Attribution." *Harv. Nat'l Sec. J.* 2 ,2011, p. 323.

③ "Damage caused by cyber activities can be diverse." Mejia-Kaiser, "Space Law and Unauthorised Cyber Activities," p.356.

using a space asset the determination of what law applies. The question becomes whether the *lex specialis* of space law is triggered by such cyber activities, or rather, do these acts constitute a use of space technology congruent with international space law. The question in relation to responsibility arises under Article VI of the Outer Space Treaty, which states:

> States Parties to the Treaty shall bear international responsibility for national activities in outer space, including the Moon and other celestial bodies, whether such activities are carried on by governmental agencies or by non-governmental entities, and for assuring that national activities are carried out in conformity with the provisions set forth in the present Treaty. . . .

This extraordinary provision gives states responsibility for at least some of the acts of non-governmental actors. The underlying policy adopted by the treaty drafters was to ensure security in space by creating incentives for states to maintain control over space activities originating from within their territory or executed by their citizens. The need for such a policy is found both in the bounds of national security concerns and in humanitarian concerns based in the dangerous nature of the technology. However, this legal language is not as expansive as it might appear at first blush. This responsibility extends to "national activities" of non-governmental actors. Even the most expansive reading of the phrase "national activities" requires there to be some minimal nexus between the state and the activity (in addition to a nexus between the state and the actor). A standard such as a state "knew or should have known" that its non-governmental entity was engaged in a space activity, would be an example of such an expansive reading. Under such an interpretation the state is responsible for space activities conducted by its non-governmental actors if it knew or should have known these activities were being engaged in. The state's knowledge thus fulfilling the requisite "national" element. Indeed, this is reinforced by the supervision and authorization clause in the next sentence, which requires states to be on constant notice of what activities its nongovernmental actors are engaging in in space. This requirement forces the state to be aware and take affirmative steps to maintain proper control of these activities.

Cyberattacks in all three of the above scenarios expose gaps in the legal parameters established under Article VI. While we are assuming that attribution is established in all three scenarios, we should nott assume that attribution is easy. Attribution can be difficult for most technologically advanced states, so it may be problematic to argue that a state should have known that a cyberattack directed at a satellite was going to emanate from within its borders.[①] That state could have been employing state of the art technology, but may not have had any notice of such an attack. The gap is found between the technology that the drafters of the Outer Space Treaty anticipated in the 1960s and the technology that actually developed in the period since then. International space law was developed on the assumption that "[t]he great cost of space exploration means that it is a matter for government appropriations."[②] Not only

---

① Clark and Landau, "Untangling Attribution."

② Eilene Galloway, "The Community of Law and Science," 1 *Proc. Coll. L. Outer Space* 62 (Andrew

did the drafters not sufficiently foresee the development of commercial space endeavors, they could not have foreseen a world in which the possibility of an anonymous individual with cobbled together hardware could ostensibly engage in a space activity. This is partly because space activities were quite literally "big" when the key principles of space law were developed. States were on notice because all they had to do was open their eyes to their territories to find notice of space activities. This is not necessarily so with a cyber attacker using compact equipment. Thus Article VI is based on technological assumptions that underlie the logic of its applicability. States were willing to accept a higher degree of responsibility for a variety of reasons, but they did not contemplate a world wherein such activities were not completely under state control.

Cyberattacks in all three scenarios challenge the once tight bounds of Article VI by breaking even the most nominal links to attribution which gives the article its teeth. Cyberattacks that engage space technology may not be attributable to the state as a "national activity." If this is the case then space law is not triggered by the cyberattack itself. This is because the nature of cyberspace creates fundamental changes to the way the technology works, and the law was not written to accommodate such changes.

This can further be illustrated by the Liability Convention. The underlying policy of the Liability Convention is to protect states and individuals from the ultrahazardous nature of space activities. Its goal is to ensure that victims receive compensation for wrongful damages. As such Launching States are liable for damage caused by their space objects under victim oriented terms.

Cyberattacks cause interpretive problems for the phrase "by a space object" found in Article II & III of the liability convention. Under these articles launching states are liable only for damage done "by" their space objects. Cyber technologies strains this little pronoun to the point of breaking. In Scenario 1, there is a gap between the space technology and the damage done. While the satellite is the critical link in the chain of events it is not a necessary link. The cyberattack could have been perpetrated through other channels. This type of attack is not space dependent and therefore it stretches "by" too far if it is interpreted to contain such attacks. This is especially so in light of the still problematic gap in attribution. Even under Article II's strict liability regime for damage to the surface of the Earth the disconnect seems broad as this is not the type of ultrahazardous damage that the treaty was drafted to guard against.

In Scenario 2, the "by" link is significantly stronger, since this time the damage is connected directly to the satellite via a communications link of some sort, yet it still has the distance problem found in Scenario 1, in that it is not the satellite that causes damage, but the information in the signal itself. While the link to the satellite feels stronger, the technical weakness to some extent still exists since the damage is still caused by information that transits through the satellite, and not the physical satellite itself.①

Scenario 3, on the other hand bridges that gap only to leave another one. In Scenario 3, the hacker uses the satellite to directly damage another satellite. In this case the triggering precondition "by" is met. However, this does not necessarily mean that there will be liability. Since such damage falls under Article III's fault based regime it

---

G. Haley & Welf Heinrich eds., Wein, Springer, Verlag, 1959.

① Mejia-Kaiser, "Space Law and Unauthorised Cyber Activities." p.360.

will need to be determined whether the launching state took reasonable precautions to ensure its cybersecurity to prove fault.[①]

III. Analytical Framework

The above analysis is meant to show how cyberspace stretches the terms of responsibility and liability under the space law regime.[②] Similar problems can occur elsewhere as cyber technology becomes further embedded in space technologies. For instance, cyberattacks can push the bounds of ITU regulations on harmful interference or influence how the law of armed conflict may apply to space assets during conflicts. Rigid loyalty to legal regimes built on different technological assumptions can lead to negative outcomes in light of underlying policy values. For instance, application of space law to Scenario 1, would result in states being subject to liability they did not contemplate when drafting the treaty for acts of which they have little notice. Below are analytic or interpretive strategies that can be of use when investigating such problems. They are 1. Balancing the values at stake; 2. Understanding the political possibilities; and 3. Engaging in technological disambiguation.

The underlying purpose of the competing legal regimes are important indicators as to how the law should be applied. In the analysis above, the underlying policy for liability is to protect individuals from harm caused by ultrahazardous space activities. This is not the type of harm examined in Scenario 1, and the fact that a harm occurred should not *de facto* require the extension of the space law regime. In this case, the strict application of space law could give states leave to limit access to satellite communications by non-governmental entities. This could lead directly to human rights violations, since such regulation is often targeted at minority political parties. The act of weighing these values against each other allows for an understanding of the possibility of the effects that choice of law could have.

The political possibilities that are available to states in these types of disputes create critical parameters that should be recognized. State's interpretation of the law often serves as a strong indicator of the law's content.[③] In the case of the Liability Convention, states have been reluctant to fully engage with the treaty in cases where it was clearly applicable.[④] This is because states see some utility in not having the terms of the Liability Convention defined, making it unlikely that states would agree to apply such law to cases such as Scenario 1 and Scenario 2. This may be especially so in the case of a major space power that could also have the political power to resist such application.

---

① *See P. J. Blount, "Satellites Are Just Things on the Internet of Things," Air and Space Law 42, No. 3, May 1,2017, pp. 273–93. But see M*ejia-Kaiser, "Space Law and Unauthorised Cyber Activities." p.365.

② It should be noted that this analysis only covered whether or not *lex specialis* rules of applied in the three scenarios. Other avenues for recovery may exist under international or domestic law.

③*See generally* Reisman, W. Michael. "International Incidents: Introduction to a New Genre in the Study of International Law." *Yale J. Int'l L.* 10 ,No.1, 1984.

④ The *Cosmos 954* incident is the only case in which the treaty is invoked. However, it better serves as an example of a state preference for avoiding application of the treaty, since at the end of the day the Treaty did not play a critical role in the outcome.. Similarly, the incident involving the collision of an *Iridium 33* and *Cosmos 2251* displays a similar preference.

Technological disambiguation involves evaluating which technology is the primary medium of a specific act. This is important because, as already noted the use of space technology is an important prerequisite for the application of space law. In all three of the above scenarios cyberspace is the initial medium, but this does not equate to the primary medium. In the first scenario, cyber is primary medium of the attack. This is because the attackers are ambivalent as to whether the attack itself travels via deep sea cables, standard telephone lines, or satellite. Space is neither the target nor the primary medium in this scenario. On the other hand, in Scenario 3 there is a definite nexus with space technology, since the goal of the attack is to disable a satellite via another satellite. Indeed the cyber portion of the attack is only a method for accomplishing an attack using a space object. Scenario 2 splits the difference between these two opposites as both technologies are mediums for the particular attack. The misinformation portion of the attack is clearly cyber, whereas the fact that the information is unique to the space object makes this a use of space technology. Technological disambiguation is limited in usefulness due to the convergence caused by cyber technologies.[①]

IV. Conclusion

This analysis highlights the fact that there is a severe lack of clarity in the law applicable to cyberattacks on, in, and through the space segment due to overlapping technological spaces. This overlap is likely to continue to intensify as information technologies become more embedded through convergence with more traditional technologies. Questions of law, especially in cases of *lex specialis* regimes, will become increasingly murky as a result. The framework outlined in this paper is meant to provide a way forward in conceptualizing and addressing such issues by recognizing that the law-technology dynamic sometimes leads to situations in which no clear answer as to applicable law exists. It is by no means a complete theory, and it requires a more rigorous evaluation in light of extant case studies and developing technology. Indeed, as other areas where cyberspace interactions are occurring are being examined, other principles may become apparent, and some may fail.

It is hoped that this brief paper can assist in establishing a deeper understanding of the workings of technology and their interactions with the law in an ever changing environment. As convergence continues, disambiguating legal spaces will become critical to understanding the disciplinary and jurisdictional limits of the law.

---

① Kulesza, *International Internet Law*, p.53.