CYA: A Legal Perspective on How to ~~do~~ Cybersecurity in Space

*P.J. Blount**

Abstract

This paper addresses the issue of cybersecurity in the context of the space environment and discusses, from a legal perspective, what it means for a space operator to be cyber-secure. This paper will argue that cybersecurity law should be understood as a governance framework constructed from a variety of documents that includes traditional legal documents, but that also relies on policies, technical standards, and technical specifications. This paper will then discuss how a lawyer is supposed "do" cybersecurity for space clients, in particular when the law itself is difficult to pinpoint.

1. Introduction

Cybersecurity in space is, to say the least, a hot issue within the space community at large and within the space law community specifically. Lawyers, though, are often overwhelmed or thwarted when they begin to dive into cybersecurity law due its lack of definition. If you type "space law" into an Internet search bar, then you are met with five treaties and numerous domestic laws that make up an identifiable body of law. When you type "cybersecurity law," the output is much less definite and substantially more technical than legal. This, of course, does not mean that there is no such thing as cybersecurity law, but it does illustrate that the legal way markers that lawyers are often comfortable with are largely missing from this body of law.

This paper will address this issue in the context of the space environment and discuss, from a legal perspective, what it means for a space operator to be cyber-secure. This paper will argue that cybersecurity law should be understood as a governance framework constructed from a variety of

* SES / University of Luxembourg, Luxembourg, pjblount@gmail.com. The views expressed in this paper are the author's own and do not represent the views of his employer or any organizations with which he is affiliated. This research is made possible by a generous Industrial Fellowship grant from the Luxembourg National Research Fund.

documents that includes traditional legal documents, but that also relies on policies, technical standards, and technical specifications. This paper will then discuss how a lawyer is supposed "do" cybersecurity for space clients, when the law itself is difficult to pinpoint.

This paper will first proceed by examining the concept of cybersecurity and discussing the specific issues that create challenges in the space environment. Next, this paper will discuss the framework of governance that lawyers need to be aware of when dealing with cybersecurity issues for clients. Third, this paper will discuss what steps lawyers need to take to ensure that their space clients are maintaining a requisite level of cybersecurity. This paper will then conclude with brief recommendations for capacity building in cybersecurity law and policy for the space industry.

2. What is Cybersecurity Law?

When an intrepid law student first plugs the term 'space law' into an Internet search engine that student is met with results that portray a complex, yet cohesive and coherent body of law. Whilst space law has plenty of offshoots into other areas of law making its boundaries fuzzy, there is consensus that the core of the field is made up of a treaty regime and a number of domestic laws and regulations. Indeed, while every teacher of space law likely teaches it very differently, one could surmise that there is some unity and large overlap as to the scope of the basic legal materials that are covered.

This is not so with Cybersecurity Law. As a field it is very difficult to identify a core set of legal documents that rise to the level of identifying cybersecurity law. There are several reasons for this. The first is that the term cybersecurity itself is fraught with fragmentation as to its definition.[1] This makes it difficult to identify the full scope of cybersecurity and its interaction with competing terms such as information security or privacy.[2] Second, and related to this, is that the law itself is fragmented and undefined.[3] Some laws such as China's cybersecurity law are directed at network operators,[4] whereas others such as the raft of cybersecurity legislation in the United States is targeted explicitly at government operators,[5] and still other laws are directed at specific types of

1 European Union Agency for Network and Information Security, *Defintion of Cybersecurity: Gaps and Overlaps in Standardization, v. 1.0* (December 2015).

2 *See for* example, NIST, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, SP-800-37, rev. 2 (Dec. 2018) 13-14.

3 *See generally*, Jeff Kosseff, "Defining Cybersecurity Law," *Iowa L. Rev.* 103 (2017): 985.

4 *See* Liudmyla Balke, China's New Cybersecurity Law and U.S.-China Cybersecurity Issues," 58 *Santa Clara Law Review* 137 (2018) and Jyh-An Lee, "Hacking into China's Cybersecurity Law," *Wake Forest L. Rev.* 53 (2018): 57.

5 *For instance* the Federal Information Security Modernization Act, Pub.L. 107–347, at Title III (2002). *See generally*, Kossef, "Defining Cybersecurity Law" and Jeff

information such as the European Union's General Data Protection Regulation.[6] In the midst of this, there is a great deal of gap filling such as the development of a common law fiduciary duty of a corporate board to maintain cybersecurity[7] or the US Federal Trade Commission's use of its enforcement power over unfair trade practices as a weapon against corporate data breaches.[8] Finally, the most marked reason for the lack of cohesiveness in defining cybersecurity law is that in reality there is very little law that tells an operator exactly what they must do to be secure. Cybersecurity regulation is technically sparse compared to other information security regulations. For example, data retention requirements can be quite precise in the form and length of retention period, whereas cybersecurity often does not go beyond the simple edict that an operator should be cybersecure.

There is of course good reason for this that emanates from a reality of legislating and regulating in the realm of innovation. Laws that give specific technological limitations are based on assumptions about how technology will work in the future, and if a single lesson can be drawn about the development of the Internet, then it is that such assumptions are rarely hardened truths. As an example, the United States Stored Communications Act of 1986[9] allows the government to access, without a search warrant, communications stored for more that 180-days on a server. This law was written at a time, when users, due to modem speeds and the per minute cost of Internet access, routinely downloaded their emails locally, and removed them from servers. The assumption underlying the law is that the user's remedy was simply ensuring that they checked their emails regularly. The underlying assumption is that this was how electronic communication would continue to work, but of course in the age of webmail, this has not continued to be the case as users lacking the same constraints as the technology of the 1980s now store and access their email on remote servers.

Cybersecurity law, as a field or discipline, is challenged by the notion of innovation, which (rightly) should make lawmakers reluctant to adopt specific technical requirements within the text of the law.[10] As an example, if a state government were to write a law stating that personal data must be

---

Kosseff, "Positive Cybersecurity Law: Creating a Consistent and Incentive Based System," 19 *Chapman Law Review* 401 (2016).

6 Regulation (EU) 2016/679: General Data Protection Regulation (2016).

7 Lawrence J. Trautman and Peter C. Ormerod, "Corporate Directors' and Officers' Cybersecurity Standard of Care: The Yahoo Data Breach," 66 *American University Law Review* 1231 (2017).

8 Kosseff, "Positive Cybersecurity Law," at 407-411.

9 Stored Communications Act, 18 U.S.C. §§ 2701–2712.

10 This can also be seen in the space context. *See generally*, P.J. Blount, "Innovating the Law: Fifty Years of the Outer Space Treaty," in Mahulena Hofmann & P.J. Blount, eds., *Innovation in Outer Space: International and African Perspectives* (Nomos 2018).

held on a server that employs AES-128 encryption, and after the enactment of this law AES-128 is broken, and the tool for breaking it becomes widely available, then operators will be forced to make a choice between compliance with the law and the safety of their data. While a legislature might have every incentive to quickly respond to such a situation, it is fair to say that lawmaking is not a quick and responsive affair, and potential changes in the law are always part of larger legislative priorities meaning that often important legislative initiatives never make it out of the drafting phase.

Since future technological developments and implementations are uncertain, legislators prefer to push technical specifications down the regulatory stack. When such rules are implemented at the level of regulations or policy then governments can be more flexible with changes. Often though, as is the case with cybersecurity, the decision is to push these rules further down into the realm of good practices, technical standards, and technical specifications. These types of 'rules' are generally nonbinding and originate either from industry or civil society. This means that the rules are flexible and can readily adapt to technological change. Additionally, the function of these types of rules, which are by and large voluntary, is not 'regulatory' in the traditional sense of creating limitations. Instead, these types of rules are evidentiary, in that compliance with them is a way for a company to evince that it was indeed adequately cybersecure for fault-based and contract-based claims. For instance, if a company is sued over or subject to an enforcement action over a data breach, a defense can be formed by showing that the company complied with technical standards and good practices in order to mitigate the risks of such an incident. If that company can show that it was compliant with, for example, the ISO 27001 on information security, then it would be difficult for a public authority or a court to rule that the data breach was a result of the company's negligence in the realm of cybersecurity.

3. Doing Cybersecurity

This leads to the question of what it means to "do cybersecurity law." This is a problem that may leave many lawyers in an uncomfortable position. This is partly because there is no legal text for them to determine whether there is compliance, and partly because the texts that do exist are technical in their specifications and therefore must be carried out by the responsible technical team within an organization. The fact is that most lawyers will not have the requisite knowledge to directly implement cybersecurity concepts. What then is the lawyer's role in the cybersecurity enterprise?

The lawyer's role in cybersecurity is actually, quite similar to the lawyer's role in other regulary and compliance areas. In short, it is CYA: Cover Your Ass or, more likely, CYCA: Cover Your Company's Ass. As indicated above, cybersecurity law is about collecting and maintaining an evidentiary record of

the organization's actions to mitigate the risk of potential cyber incidents. This involves among other things: participating in the risk assessment and development of the risk mitigation plan, managing the documentary evidence that a cybersecurity plan has been implemented, and maintaining compliance over time in light of changing law and technology. This is, of course, in addition to ensuring compliance with any domestic regulations that touch on data security, information security, or cybersecurity as well as contract elements touching on the same. It is important to remember that this is not a task that sits solely in the lawyer's dossier. Rather, cybersecurity is a partnership between the legal regulatory and compliance office and the cybersecurity or information security team of a given entity.

An example of how this might work can be found using the International Standards Organization 27001 standard on Information Security Management and the surrounding 27000 family of standards.[11] This standard helps to identify areas of risk to information security and identify and adopt measures to mitigate that risk through a list of controls that can be selected. ISO 27001 has a two important attributes that are important to adopting a cybersecurity plan for an entity. First, is that it recognizes that cybersecurity is not one size fits all. Instead, it is a bespoke process that is driven by a number of factors such as location of the company, the types of information systems it employs, the types of data that it handles, and myriad other factors that influence the risk profile of a particular entity. This means that the standard itself is flexible and adaptable to the specific needs of the entities that are intending to implement it. Second, it recognizes the value in creating and evidentiary record of information security actions. It is not simply enough for a company to say that it has implemented ISO 27001, that company will need to be able to show through policies, contracts, logs, and a variety of other artifacts that it has indeed implemented the necessary controls. It should be noted that a criticism of ISO 27001 is that its implementation can be burdensome on medium and large companies thus extraordinarily so on smaller companies. Of course, ISO 27001 is not the only standard available and each entity can tailor its cybersecurity plan to its own risk mitigation needs. For instance, a similar yet lighter standard can be found in AIA's National Aerospace Standard 9933.[12] It is not a matter of what plan you choose. It is, rather, a mater of showing that you adequately identified risks and adequately took action to mitigate those risks to an acceptable level. These types of standards serve as guides in that endeavour.

11 ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements (2013) https://www.iso.org/standard/54534.html.

12 Aerospace Industries Association, NAS9933: Critical Security Controls for Effective Capability in Cyber Defense (November 2018).

The lawyer's role is not limited to simply collecting the evidence of the technological implementations, but also advising on the legal requirements that should be fulfilled by these implementations. While there isn't a cohesive body of cybersecurity law, there are numerous pinpoints of law that can influence cybersecurity requirements, many of which relate to the broader topic of information management. For instance, data protection laws such as GDPR, create requirements that particular types of data – in the case of GDPR, Personally Identifiable Information – are protected from breach. Thus, when formulating a cybersecurity plan, this should be taken into account when assessing and mitigating risk.

The lawyer's role in cybersecurity, is not completely disconnected from the text of the law, but many of the lawyer's tasks in this enterprise will be ensuring documentation that the organization was behaving as a reasonable actor in administering its cybersecurity plan. It should be emphasized here, that no system, or no usable system, is ever 100% secure. The goal is instead to manage the risk and document this in such a way that a court or enforcement agency can determine that the organization was cybersecure enough.

4. Cybersecurity in Space

Cybersecurity for space organizations will generally follow the same pattern as cybersecurity within any other organization. Indeed, for day to day business operations the cybersecurity concept employed would not likely be significantly different in form or scope from a similarly situated organization. That is not to say that space does not change the cybersecurity equation. It does, but not dramatically so. Adding space into the cybersecurity mix, means that risk managers (including lawyers) need to be able to do a risk assessment of the spacecraft and associated ground infrastructure and implement solutions to mitigate that risk adequately. This is true of any industry deploying novel technologies.

What this means in practice is that when an organization is developing spacecraft and their associated systems they should be developing with security by design in mind, including cybersecurity. This will, of course, be dependent on the particulars of the specific spacecraft. It goes without saying that the cybersecurity requirements for a university launched cubesat with a relatively short lifespan will be dramatically different from a GEO satellite designed to carry national security communications. The risk assessment will have to take into account the capabilities and physical location of the spacecraft and its associated ground stations and implement cybersecurity that is appropriate for that craft.[13]

13 The author has a second paper at the 2020 IAC dealing with this problem. *See*, P.J. Blount, "Cyber-Risk Assessment in the Space Domain: Categorizing Cyber-Risk Across Space Operations," IAC 2020 Cyber Edition, Session E9. 2/D5.4 (2020).

The bad news is that there is not much guidance out there in terms of how to do this. There is no ISO 27001 for developing an information security plan for spacecraft. However, some work has been done. As mentioned above the AIA has released a cybersecurity standard for the aerospace industry, but the standard itself is geared more towards general information security and not the cybersecurity of aerospace objects.[14] The closest that one can get to a cybersecurity standard tailored to the space enterprise is the US Committee on National Security Systems' (CNSS) Space Platform Overlay.[15]

The CNSS overlay is a space specific overlay for NIST standard 800-53, which lays out security controls for US federal information systems.[16] What this means is that the CNSS document can be "overlaid" onto the NIST document to adapt it to the space context. Both of these documents, though, are concerned with information management in the US federal system, and as its name implies the CNSS standards are directed at systems carrying sensitive national security information. What this means is that while the CNSS Space Overlay is an interesting starting point for thinking about developing a security concept for a space system, its national security context may make it burdensome to implement for non-national security operators.

The question of what is cyber-secure enough in the space domain is still open and there is little formal guidance that is specific to the space industry. As a result, the legal and cybersecurity teams that are working to create the security concept for a specific system will have little formal, industry specific guidance on how to identify and mitigate risks during their risk assessment. Rather, there is a patchwork of documents that make an incomplete picture for responding to security risk for space systems. This fundamentally makes the CYA enterprise a difficult one for the space domain. A risk averse strategy can needlessly increase cost, but a risk acceptance approach can create risks to the mission as well as for other operators. It is this collective action problem that increases the need for industry specific guidance on cybersecurity.

5. Building Capacity

The fact that cybersecurity is a hot topic in the world of space is a positive force because there is a distinct need for collective industry action to help

14 Aerospace Industries Association, NAS9933.

15 Committee on National Security Systems, Space Platform Overlay, CNSSI no. 1253 Attachment 2 to Appendix F (2014). *See also*, Committee on National Security Systems, National Information Assurance Instruction for Space Systems Used to Support National Security Missions, CNSSI No. 1200 (2014).

16 National Institute of Standards and technology, *Special Publication 800-53, rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations* (2015).

define how operators should approach cybersecurity of space systems.[17] It is important to note that this is not a call for "cybersecurity law" for the space industry. Cybersecurity in space is not yet ripe for regulation and will, for the foreseeable future, legally speaking, be the subject of private law, namely contracts and private disputes. The cybersecurity lawyer is not a lawyer focused on regulations but on ensuring that an evidentiary body has been created that protects the space operator from potential claims resulting from a cybersecurity incident.

The development of industry specific standards and guidance will, like in other industries, need to be predicated on information sharing among industry actors on threats and vulnerabilities that various space systems perform. There have been a number of formative efforts at pursuing such information sharing. The most prominent to date has been the US led Space Information Sharing and Analysis Center (Space ISAC). The Space ISAC "serves to facilitate collaboration across the global space industry to enhance our ability to prepare for and respond to vulnerabilities, incidents, and threats; to disseminate timely and actionable information among member entities; and to serve as the primary communications channel for the sector with respect to this information."[18] Such collaborative efforts help to build industry understanding that individual operators can use to develop system specific security concepts.

There is also a need for standards bodies, such as ISO or IEEE, to begin the work of developing technical standards for space systems and space subsystems in order to help the industry better respond to threats from cyberspace and to help these companies CYA. The lawyer's role is to ensure that the organization's response to cybersecurity risks is adequate in the sense that it would survive a challenge in court or administrative hearing. Such showings rely on producing evidence that the technical team implemented the necessary controls, but at present as outlined in this paper, there is little understanding of what controls should be implemented.

Cybersecurity will remain a challenge for all industries for the foreseeable future and the space industry is no exception. However, because space is a strategic domain, the risk that results from vulnerabilities will be unevenly spread. A common vulnerability could interfere with entire classes of satellite or a vulnerability on a single satellite could result in that satellite causing interference with other activities. The commercial actor in this situation needs to be able to effectively determine and apply controls to ensure a reasonable level of cybersecurity is implemented within a given system.[19] The lawyer's

17 Gregory Falco, *Job One for Space Force: Space Asset Cybersecurity* (Belfer Center for Science and International Affairs, 2018).

18 Https://s-isac.org/mission/.

19 This is specifically required in the Trump Administration's SPD-5: Cybersecurity Principles for Space Systems (4 September 2020).

role in this enterprise is to CYA by ensuring that a record of the operator's mitigation and compliance efforts is maintained in case of a cybersecurity incident.

6. Conclusion

Cybersecurity is a problem that does not have a simple, silver bullet solution. Instead, it is a developing and dynamic problem that will be faced by nearly all industries globally. As the digitization and networkification of devices and infrastructure continues, so too will new threats and vulnerabilities advance and multiply. The space industry needs to recognize that this is a common problem that necessitates some level of collective action in response. Despite the current lack of clarity in rules, methodologies, and good practices for maintaining cybersecurity in the space domain, the cybersecurity lawyer will still need to ensure that the organization they represent covers its ass by building a record of risk assessment and mitigation in the cybersecurity context.