Kerberized Identity-Based Encryption and the Interoperability of Space-Based Systems

by William Harrison Loucks

B.S., Mathematics and in Electrical Engineering and Computer Science, Massachusetts Institute of Technology, 2018

Submitted to the
Department of Electrical Engineering and Computer Science
in Partial Fulfillment of the Requirements for the Degree of

Master of Engineering in Electrical Engineering and Computer Science

at the

Massachusetts Institute of Technology

May 2019

Author: ______________________________
Department of Electrical Engineering and Computer Science
24 May 2019

Certified by: ______________________________
Dr. R. David Edelman
Director, Project on Technology, Economy, and National Security
24 May 2019

Certified by: ______________________________
Dr. Robert M. Denz
Secured and Assured Systems, Draper Laboratory
24 May 2019

Accepted by: ______________________________
Dr. Katrina LaCurts
Chair, Master of Engineering Thesis Committee
24 May 2019

Kerberized Identity-Based Encryption
and the
Interoperability of Space-Based Systems

by William Harrison Loucks
Submitted to the Department of Electrical Engineering and Computer Science

May 24, 2019
in Partial Fulfillment of the Requirements for the Degree of
Master of Engineering in Electrical Engineering and Computer Science

Abstract

This study presents a key management protocol for satellite communication which jointly considers features of the environment that may preclude existing asymmetric key exchanges and international legal instruments which may direct the most optimal form of cross-constellation third-party authentication within a global common. The approach, titled Kerberized Identity-Based Encryption (KIBE), utilizes aspects of Kerberos and identity-based encryption to establish a shared key, encrypt a message, and authenticate both of the aforementioned in a single transmission without the need for assets to share predistributed cryptographic material. KIBE is implemented using a network in which low-resource computers can simulate cross-constellation communication and mutual authentication using a trusted third-party. Lastly, this study illustrates how KIBE may be utilized to support an infrastructure of secure space-based communication systems as a result of cryptographic coordination with an internationally trusted entity to subsequently promote broader compliance with the international rule of law in outer space.

Advisers: R. David Edelman and Robert M. Denz

Acknowledgments

Thank you to my family and friends. Without your support, my experiences in so many areas would be far different. Thank you to Dr. R. David Edelman for his feedback and insights into the realm of international policy and national security throughout the writing of this paper. In addition, thank you to Dr. Rob Denz, Mike, Rubens, and all of the other engineers at Draper Lab who assisted me with my projects throughout the year and afforded me the opportunity to get to know them.

All statements of fact, opinion, or analysis expressed are those of the author and do not reflect the official positions or views of the U.S. Government. Nothing in the contents should be construed as asserting or implying U.S. Government authentication of information or endorsement of the author's views.

Contents

1 Introduction 9

2 Protected Satellite Communication 15

2.1 Confidentiality 15

2.2 Integrity and Authenticity 18

2.2.1 Replay and Denial of Service Attacks 22

2.3 Key Management 23

3 Space as an International Domain 32

3.1 International Legal Framework 33

3.2 Modern Asset Deployment 58

3.2.1 Case Study: Undersea Cables 68

3.2.2 Satellite-to-Satellite Compatibility 74

4 Kerberized Identity-Based Encryption (KIBE) 80

4.1 Identity-Based Encryption 82

4.1.1 Bilinear Pairing 89

4.1.2 Boneh-Franklin Identity-Based Encryption 92

4.2 Kerberos 95

4.3 Prior Work 97

4.4 Kerberized Identity-Based Encryption (KIBE) 100

5 A System for Registration 110

5.1 A Collection of Consortiums 118

6 Conclusion 126

List of Figures

1 Bit security comparison between symmetric and asymmetric algorithms. Paar, C, Pelzl, J. *Understanding Cryptography.* Berlin Heidelberg: Springer, 2010. pp. 156. 21

2 KIBE flow of information in a two-party example. 104

3 Time complexity of encryption for implementation of Boneh-Franklin using the Tate pairing, given a security parameter for the elliptic curve. 108

4 Time complexity of decryption for implementation of Boneh-Franklin using the Tate pairing, given a security parameter for the elliptic curve. 108

5 Ciphertext length in bits for implementation of IND-ID-CPA and IND-ID-CCA Boneh-Franklin using the Tate pairing, given a security parameter for the elliptic curve. Message in $\{0,1\}^{256}$ and Verification String in $\{0,1\}^{128}$.109

1 Introduction

Affairs in outer space demand a contemporary infrastructure to address the objectives of international state and non-state actors. Sustaining adherence to international directives can be as difficult to support in outer space as in any other global common. However, activities in outer space enjoy significant differences from operations at sea, and to an extent, in the air. Distinct commercial and state actors may seek to deploy thousands of autonomous satellites that intentionally achieve degrees of interoperability, enabling disparate constellations to transact or support the regular services of one another. In contrast to vessels at sea and manned aerial vehicles, which communicate through human interaction or existing network protocols, outer space offers an environment and a necessary level of asset autonomy which likely preclude frequent human intervention and the use of widely employed network techniques. Notably, the mechanism to autonomously authenticate communication between spacecraft not only presents an opportunity for a technical solution, but also illustrates a gap that an international body may have to fill in order to legitimize tools for third-party authentication. As a result, this study is twofold, first suggesting a key management protocol to enable confidential and authenticated communication between distinct constellations, and second, recommending a new, consortium-based international system for cross-constellation interoperability and cryptographic coordination between space objects. The product could be an infrastructure which supports broad network interoperability between distinct space-based assets and facilitates wider adherence to the existing international rule of law in outer space.

Lighter and reusable launch vehicles, satellite miniaturization, and an industry of commercial competitors allow additional actors to feasibly position assets in orbit to meet national security, civil, and economic objectives. For instance, global commercial entities supported a nearly $384 billion space economy in 2017, which the United States (U.S.) Chamber of Commerce estimates will exceed $1.5 trillion by 2040.[1] In addition, U.S. armed forces routed 90% of communication through satellites during the 1991 Gulf Conflict – roughly 50% of which passed through commercial systems – and by 2003 possessed approximately 30 times the available bandwidth from satellite constellations.[2] By 2020, some estimate that U.S. Department of Defense (DOD) bandwidth requirements may rise to approximately 70 times the 2003 availability, deepening an existing reliance on satellite capabilities.[3]

While satellite deployment has become ubiquitous for military and civilian use, systems lack standard tools to address information security in view of networks formed by space-based assets, causing constellations to operate in isolation over independent networks. Namely, features of cross-link communication over ad hoc networks such as propagation delay, intermittent connectivity, sparse bandwidth availability, and limited hardware resources likely preclude asymmetric key exchanges typically utilized over the Internet, requiring devices to store predistributed cryptographic material or communicate devoid of encryption entirely.[4] The product is a mesh of independent networks, each of

[1] Higginbotham, B. "The Space Economy: An Industry Takes Off." U.S. Chamber of Commerce, Above the Fold. Oct. 11, 2018. During the same time, Goldman Sachs and Morgan Stanley analysts predict the industry will exceed $1 trillion and Bank of America Merill Lynch analysts expect the industry to reach $3 billion. *Id.*

[2] Wilson, T. "Threats to United States Space Capabilities." Prepared for the Commission to Assess United States National Security Space Management and Organization. *Federation of American Scientists.* Jan. 2001; Joe. L., Porche, I. "Future Army Bandwidth Needs and Capabilities." RAND, Arroyo Center. 2004.

[3] A RAND report asserts that DOD requirements will move from 1.9 Gbps in 2002 to 137.5 Gbps in 2020. *Id.* See also the transition from roughly 7 Defense Satellite Communications System (DSCS) satellites to over 10 Wideband Global SATCOM (WGS) satellites, where one WGS satellite provides more bandwidth than the entire DSCS constellation – thus, roughly 70 times the bandwidth. U.S. Air Force Fact Sheet. "Defense Satellite Communications System." Nov. 23, 2015. https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104555/defense-satellite-communications-system/; U.S. Air Force Fact Sheet. "Wideband Global SATCOM Satellite." Mar. 22, 2017. https://www.afspc.af.mil/About-Us/Fact-Sheets/Display/Article/249020/wideband-global-satcom-satellite/.

[4] Consultative Committee on Space Data Systems. "Space Missions Key Management Systems." ch.

which may be highly affected by disruption to a single asset. As a result, this study first assesses the impact of environmental features on the design of a key management protocol for cross-constellation communication – a step toward enabling robust interoperability with meaningful information security. Then this study transitions to examine how the existing international legal regime may govern the mechanism by which assets are electronically authenticated over the air in a global common.

The United Nations (UN) is likely the most appropriate body to guide the behavior of actors in outer space, including the identification and authentication of spacecraft with transborder provenance. The Preamble of the Charter for the United Nations asserts that the forum intends "to establish conditions under which justice and respect for the obligations arising from treaties and other sources of international law can be maintained," and President Dwight D. Eisenhower's statements regarding the world body in 1953 are just as prophetic today: "Never before in history has so much hope for so many people been gathered together in a single organization."[5] The UN likely endures because of a historic international commitment to representation and reverence for its ideals, establishing itself as the preeminent entity to govern global domains such as outer space.

Further, functional agencies within the UN, such as the International Telecommunications Union (ITU), serve as venues within the world body to handle specialized issues of a narrow scope. In particular, the ITU compiles the broadcast frequency bands registered by states and international organizations to limit interference between distinct systems.[6] Here, international actors generally operate within their dedicated frequency

4.2. Nov. 2011. https://public.ccsds.org/Pubs/350x6g1.pdf.

[5] Charter of the United Nations, preamble, Jun. 26, 1949; Eisenhower, D. "Atoms for Peace Speech." Dwight D. Eisenhower Presidential Library, Museum and Boyhood Home, Press Release. Dec. 8, 1953. https://www.eisenhower.archives.gov/research/online_documents/atoms_for_peace.html.

[6] Constitution and Convention of the International Telecommunication Union, Oct. 1, 1994, 1825 U.N.T.S. 330.

ranges, consistently interpret the language of the Constitution and Convention of the ITU, and comply with the provisions therein likely due to a well-acknowledged benefit in obtaining the exclusive right to particular frequencies. However, the lack of textual ambiguity and robust acceptance enjoyed by ITU provisions are not observed with all international instruments, including those that promote the reliable, sustainable use of outer space.

As President Harry S. Truman noted in his address at the 1946 opening session of the United Nations General Assembly: "[t]he difficulty is that it is easier to get people to agree upon peace as an ideal than to agree upon principles of law and justice or to agree to subject their own acts to the collective judgment of mankind."[7] Still today, provisions to administer order in global commons suffer from perennial issues associated with treaties of all kinds, including varying degrees of compliance and a lack of instruments for international enforceability.

With respect to outer space, this paper primarily examines the Treaty on the Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies ("Outer Space Treaty"), which has been ratified by 109 UN member states since 1967 and remains the most comprehensive international legal framework for outer space.[8] However, certain provisions in the Outer Space Treaty – such as those which require states to continually supervise public and commercial activities under their purview and those which assign liability to states for all such pursuits – have yet to be rigorously defined, tested, and ultimately practiced.

[7] Truman, H. Address in New York City at the Opening Session of the United Nations General Assembly. Harry S. Truman Presidential Library and Museum, Public Papers. Oct. 23, 1946. https://www.trumanlibrary.org/publicpapers/index.php?pid=914.

[8] United Nations Treaty on the Principles Governing the Activities of States in the Exploration and Use of Outer Peace, including the Moon and Other Celestial Bodies, art. 7, Jan. 27, 1967, 610 U.N.T.S. 205; United Nations Committee on the Peaceful Uses of Outer Space, Legal Subcommittee, Status of International Agreements Relating to Activities in Outer Space as at January 2019, Apr. 1, 2019, A/AC.105/C.2/2019/CRP.3.

Nevertheless, as state and commercial actors deploy vast amounts of assets, UN affiliation could promote and legitimize regulations which states may choose to build into their own legislation, including cryptographic registration. Moving forward, state and commercial actors may deploy assets designed to function in isolation, especially those dedicated to national security, but the operational and legal advantages associated with cross-constellation capabilities may adjust this model. Agreements between combinations of state and non-state actors to maintain compatible infrastructures may not only provide inter-system redundancy, but also minimize the existing burden of continued supervision pursuant to the Outer Space Treaty, reduce operating costs, limit resultant debris generated, and diminish the likelihood of collisions – all of which presumably rest in the interests of actors hosting space-based services.

In view of the modern deployment of space-based assets and the governing legal instruments, this paper then introduces a case study on undersea cables which provide a paradigm with aspects that may be translatable to outer space. For instance, cable operators intentionally retain available bandwidth on their networks to flexibly assume traffic from partner lines, providing persistent service even if a line is damaged. Moreover, undersea cables are operated and maintained by commercial entities, but the domain within which they primarily reside and their interactions with vessels at sea are governed by an international legal regime, analogous to satellite systems. In cases where external redundancy is desired to support the resiliency of independent services, the undersea cable sector teaches that such redundancy is facilitated through technical interoperability and a widely recognized rule of law.

After assessing the extent of interoperability espoused by undersea cable systems and the existing legal framework which may determine the origin of over the air third-party authentication, this paper presents a new key management protocol. The approach, titled Kerberized Identity-Based Encryption (KIBE), uses identity-based asymmetric cryptography and a variant of Kerberos to allow satellites to exchange a symmetric key, encrypt a message, and authenticate the aforementioned in a single transmission. In addition, satellites do not need to share any overlapping cryptographic material before instantiating communication, and public keys do not need to be redistributed to every satellite for forward secrecy. Moreover, according to Consultative Committee for Space Data Systems (CCSDS) – a body which studies space communication standards, comprising 11 international agencies, including NASA and ESA – recommendation and consideration for maximum security, symmetric key cryptography is employed to the extent possible.[9] However, unlike the Kerberos protocol, no third-party key distribution center is provided an inherent escrow.

The result is an approach which an international coalition of partners may utilize to authenticate one another over an infrastructureless space-based network. This study concludes by discussing how the protocol can enable a collection of consortiums to cryptographically register satellites prior to launch for third-party authentication. The section illustrates how identity-based encryption and cryptographic registration, coupled with the physical interoperability observed in the undersea cable sector but considering the nuances of operating in outer space, may allow satellite operators to create an infrastructure of communicating nodes in orbit. The resultant infrastructure may support an interconnectedness that increases the resiliency of each service and addresses concerns pursuant to the Outer Space Treaty and any future instruments which may limit the number of assets deployed to the minimum required to provide a service.

[9] Consultative Committee on Space Data Systems. "Symmetric Key Management." Jun. 2018. https://public.ccsds.org/Lists/CCSDS%203540R1/354x0r1.pdf; For members list, see: https://public.ccsds.org/default.aspx. Accessed: May 2019.

2 Protected Satellite Communication

Civilian and military up-, down-, and cross-link satellite communication will require encrypted channels for end-to-end security. However, network techniques utilized over the Internet may be suboptimal for use between space-based systems which must communicate over large distances with low data throughput.[10] As a result, there may be a fundamental need to develop new network protocols which deliver Internet-like services with equivalent speed, fidelity, and security. The latter of which is the focus of this study.

Direction finding, traffic analysis, and cryptanalysis can each play decisive roles in disrupting protected communication between nodes. Therefore, to defend space-based information systems against sophisticated adversaries, one may address the following broad concerns: confidentiality, integrity and authenticity, and key management in view of features presented by the environment, such as limited bandwidth and intermittent connectivity between assets within a network that outer space is likely to support.

2.1 Confidentiality

Confidentiality in broadcast satellite communication has two components: discretion in traffic between a satellite and any other device, and secrecy of the information within a transmitted message packet. Regarding the former, larger wavelengths entail less focused radiative beams, increasing the ability of an adversary to discover the simple fact that communication is occurring. On the other hand, the same drawback allows systems to

[10] Consultative Committee on Space Data Systems. "Space Missions Key Management Systems." ch. 4.2. Nov. 2011. https://public.ccsds.org/Pubs/350x6g1.pdf.

transmit information to many devices over a large area, possibly masking devices which are intended to receive certain broadcasts. In sum, while a coordinated effort to mitigate traffic analysis may be a security parameter within any communication network, the effort is nevertheless rendered ineffective if the streams of communication in question are not encrypted.

In most cryptosystms, each party in the conversation holds a cryptographic key which allows them to encrypt and decrypt communication for confidential interpretation. Ideally, an observer without such a key who intercepts the transmitted data will be unable to distinguish the ciphertext, or encrypted plaintext, from a string of randomly chosen elements. Protecting against a passive adversary, who is only able to observe encryptions in transit, is characterized as semantic security.

Semantic Security. Assume probabilistic polynomial time (PPT) algorithm D is given the ciphertext $Enc_k(m)$ and outside information $h(m)$ about plaintext m. Also assume that PPT algorithm D' is given only $h(m)$. The following must hold to achieve semantic security:

$$|Pr[D(Enc_k(m), h(m)) = m] - Pr[D'(h(m)) = m]| < \epsilon,$$

where ϵ is negligibly small.

In other words, observing the ciphertext provides only negligible advantage when attempting to ascertain the plaintext in light of the context of the communication. In meeting this bar, the cipher meets the most minimal definition of security. Depending on the attack model, the entire method of encryption might require additional features. For instance, an adversary may be able to adaptively query an actor to transmit a message for which the adversary knows the plaintext – an adaptively chosen plaintext attack. Defeating this type of attack, and others, such as chosen ciphertext attacks, requires additional measures.[11]

Rijndael is likely the world's most widely used cipher, which NIST minted as the Advanced Encryption Standard (AES) in 2000 and later standardized in Federal Information Processing Standards (FIPS) Publication 197 as the official symmetric key algorithm of the U.S. government.[12] The AES algorithm is a pseudorandom function that is efficiently invertible only if one possesses the key used to generate the image of the function. Otherwise, there does not exist a known analytical or efficient algorithm to invert the AES function.

Operationally, AES encrypts plaintext blocks of a specified size, generating blocks of ciphertext after each iteration. Notice a potential security flaw with this process. Assume the message contains blocks $A|B|C|D$ which become $W|X|Y|Z$ after applying AES. If the next message is $A|B|C|E$, with $E \neq D$, the plaintext will lead to ciphertext $W|X|Y|Z'$, where $Z \neq Z'$. Thus, if an adversary intercepts both messages, he may gain knowledge regarding the first three quarters of the second message – namely, the majority of the second message is identical to the previous message. Further, the scheme is deterministic, diminishing semantic security. To diffuse changes in the message throughout the entire ciphertext, AES is coupled with what is known as a block cipher mode. Different modes vary, but secure modes provide a process for linking individual blocks of generated ciphertext such that small changes in plaintext are diffused throughout the resultant ciphertext. Further, at least the first block intakes a random vector in order to cultivate

[11] For details regarding chosen plaintext and chosen ciphertext attacks, see: *infra* notes 176-177.

[12] National Institute of Standards and Technology, Computer Security Resource Center. "Cryptographic Standards and Guidelines." Last updated: Oct. 10, 2018.
https://csrc.nist.gov/projects/cryptographic-standards-and-guidelines/archived-crypto-projects/aes-development; National Institute of Technology and Standards. Notice, 66 FR 63369. Dec. 6, 2001.

the nondeterminism required.

AES, coupled with a context-specific block cipher mode, is likely the world's most widely used cryptosystem. In addition, manufacturers, such as Intel, Raytheon, Texas Instruments, Advanced Micro Devices, and others produce microprocessors to incorporate specific instructions which make AES as efficient as possible. Further, extensive practice implementing the cipher likely enhances security against side channel attacks which may arise from inexperienced use. Thus, for confidentiality, AES has a strong advantage over many other algorithms.[13]

Communication involving systems in outer space – even if approaches to achieve meaningful security are distinct from ground-based methods – likely demand the same confidentiality afforded by algorithms such as AES. In some cases, satellites may need to encrypt messages using such algorithms before up-, down-, and cross-link transmissions. Alternatively, parties simply using the satellite system as an apparatus to carry communication may negotiate keys independently from the transport mechanism. In either case, effective tools to ensure the integrity and authenticity of communication between links within the transport apparatus may determine the overall security of the system.

2.2 Integrity and Authenticity

Message integrity and authenticity are likely to be verified by the responding satellite with a single instrument. Message integrity refers to a security property where the message has not been malleated, or altered, in transit. To attack data in transit, an adversary may attempt to invert carefully selected bits of ciphertext. For instance, a message con-

[13] Note, AES is a symmetric key algorithm, meaning that all users must have the same key in order to encrypt and decrypt successfully. Distributing the key securely to all trusted users is in the purview of key management.

taining the fragment *10* could be intentionally altered to *100*, or *"do"* altered to *"do not."* To maintain message integrity, actors may employ one of a suite of tools, which includes message authentication codes (MAC), hash-based message authentication codes (HMAC), and digital signatures.

MACs and HMACs are hoped to be one-way functions which produce a unique tag, or a compressed but pseudorandom representation of the message.[14] The initiator in a thread of communication may apply a MAC or HMAC function to the ciphertext and transmit the generated tag along with the ciphertext. The receiver then applies the same MAC or HMAC to the received ciphertext in order to verify that the message has not been altered during transmission.

Note, the above provides only limited measures to authenticate the message. For instance, an adversary can send any chosen ciphertext, apply the MAC or HMAC – so long as the function is public – and transmit a message that the receiver will attempt to decrypt. Even if the resultant message does not have semantic value, the receiver could be inundated with what he believes are valid messages. In order build a tool for authentication, MACs and HMACs may be keyed with a shared secret. Here, the initiator generates a tag as before, but the tag depends on both the ciphertext and the shared secret. As a result, only a receiver with the shared key will be able to assess the validity of a particular message. However, negotiating a shared secret for MAC and HMAC use may apply an unsupported layer of key exchange. As a result, systems may utilize asymmetric digital signatures.

To sign a message using a digital signature, a user, armed with a public-private key

[14] Perfect one-way functions are not known to exist. However, hash functions are assumed to be one-way based on the hardness of inverting the image of the function to obtain corresponding pre-image elements.

pair, applies his private key to the ciphertext, producing a signature.[15] The generated signature can be verified through a receiver's application of the first user's public key, as below:

Alice **Bob**

$(pk_A, sk_A), m$ (pk_B, sk_B)

$$\xrightarrow{\sigma = Sign(sk_A, m)}$$

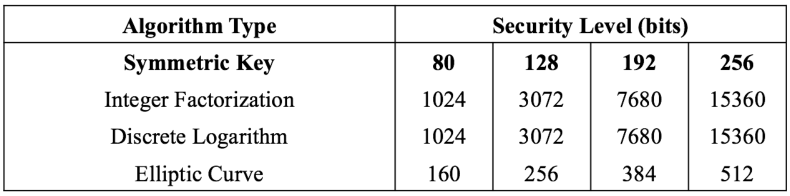
$$m = Verify(pk_A, \sigma)$$

where (pk_A, sk_A) and (pk_B, sk_B) are Alice and Bob's public-private key pairs, respectively, and m is the message to be signed.

Verifying the credibility of public-private key pairs is a distinct issue. For instance, Eve may sign a message to Bob using a random, valid public-private key pair and claim to be another party, such as Alice. In practice, a third party must certify Alice's public-private key pair in order to prevent an adversary from stealing her identity.

Space-based systems are likely reluctant to allocate time and power to encryption. Thus, algorithms for message integrity and authenticity may be resource-conscious. Asymmetric protocols, such as digital signatures, require taxing modular arithmetic and consume far more time than symmetric methods. Further, the security assumptions underlying public-key cryptography are often considered weaker than those bolstering algorithms like AES. Figure 1 below depicts the relative securities of symmetric key cryptography and the three most popular asymmetric security assumptions.

[15] Often, parties hash the ciphertext to produce a digest of the message. Then the digest is signed with his private key. This allows users to sign longer messages with the same latency and security. For a more thorough discussion on public-key cryptography, see *infra* note 20.



Algorithm Type	**Security Level (bits)**			
Symmetric Key	**80**	**128**	**192**	**256**
Integer Factorization	1024	3072	7680	15360
Discrete Logarithm	1024	3072	7680	15360
Elliptic Curve	160	256	384	512

Figure 1: Bit security comparison between symmetric and asymmetric algorithms. Paar, C, Pelzl, J. *Understanding Cryptography.* Berlin Heidelberg: Springer, 2010. pp. 156.

With respect to symmetric key cryptography, assuming λ represents the number of bits in the key, an adversary requires at most 2^{λ} guesses to identity the key through brute-force. This type of search may be the best analytic cryptanalysis which adversaries can perform against symmetric algorithms, such as AES. However, the mathematical relationship between public and private keys in asymmetric cryptography allows for powerful algorithms, such as the quadratic sieve for integer factorization and index calculus for discrete logarithms, to undermine security. Regarding elliptic curves, the MOV reduction shown by Menezes, Okamoto, and Vanstone illustrates that computing the logarithm over some elliptic curves is sometimes no harder than computing the discrete logarithm in a finite field, causing certain curves to be susceptible to index calculus attacks.[16]

Nonetheless, even without effective cryptanalysis, adversaries can simply disrupt the system's ability to process valid information. For example, replay and denial of service attacks, analogous to jamming, may be exceedingly effective at slowing a satellite's data ingress if authentication consumes significant time and power.

[16] Menezes, A.J., Okamoto, T., Vanstone, S.A. "Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field." *IEEE Transactions on Information Theory*, vol. 39, pp. 1639-1646. Sept. 1993.

2.2.1 Replay and Denial of Service Attacks

To overload receiving ports on the satellite, an adversary may send false messages for the satellite to attempt to authenticate. The effect of such an attack may delay service for valid queries. Alternatively, the adversary may *replay* a previously valid message, hoping to institute a chosen response. For instance, if Alice sends Bob a message to maneuver to the left, an adversary may be able to intercept the message and send the same instruction at a later time, possibly causing Bob to perform a similar action. In practice, a satellite may be used to provide service to dedicated regions, specified by the operator. Thus, if an adversary wishes to divert service from a given location, he may replay valid instructions to cover a disparate area.

First, to protect against overloading receiving ports with seemingly valid messages, practitioners may wish to employ an efficient authentication scheme. As noted, digital signatures, with requisite modular arithmetic, contain far more complexity than symmetric methods, such as MACs and HMACs. However, MACs and HMACs introduce issues in key distribution, as they both demand predistribution of a symmetric key. Nonetheless, a symmetric form of authentication would be strictly preferred from a perspective of protecting against receiver overloading-type attacks.

To protect against replay attacks, practitioners often introduce an expiration to authenticated messages. The expiration, or timestamp, must be encrypted – otherwise a message can be appended with any chosen timestamp. Timestamping does not adequately protect against the aforementioned overloading-type attacks. However, timestamping does prevent a receiver from decrypting a message and acting on the plaintext. For instance, taking the above example, if Bob timestamps his message to expire at time

t, an adversary who replays the same message at $t + \epsilon$ will not successfully convince Alice to act on the message.

If an actor is concerned that an adversary may quickly replay the message before t, different forms of labeling may be employed. As an easy fix, one can encrypt a random counter and ensure that the receiver does not act on messages which contain the same counter. In this case, the adversary, even if he knows the counter, would need knowledge of the secret key in order to build a convincing message.

In the end, an algorithm for authentication – especially if authenticity is confirmed before decryption is attempted – should be as efficient as possible in order to mitigate denial of service attacks. Further, some form of timestamping could be incorporated in order to prevent replay attacks. This paper's protocol will attempt to maximize efficiency using a symmetric method for authentication where possible; however, with symmetric key cryptography, the issue becomes coordinating the secure distribution of cryptographic material to all relevant parties.

2.3 Key Management

Existing mechanisms to negotiate shared cryptographic material for confidentiality, integrity, and authenticity can require high degrees of interaction or material predistribution, likely contributing to the CCSDS's statement that "[s]pecial environmental constraints exist in the space domain and they pose specific challenges for the development of key management solutions."[17] Many asymmetric protocols, such as those utilized over the Internet, require a noticeable amount of information exchanges in order to es-

[17] Consultative Committee on Space Data Systems. "Space Missions Key Management Systems." ch. 4.2. Nov. 2011. https://public.ccsds.org/Pubs/350x6g1.pdf.

tablish a shared secret key, presenting challenges for assets which experience intermittent connectivity and noticeable propagation delay associated with communication over large distances.[18] Further, while symmetric key cryptography could address most of these network concerns, but predistribution of cryptographic material requires all communicating parties to trust a key distribution center (KDC). This inherently delivers an escrow to the KDC and possibly allows the compromise of one spacecraft to spread to other assets, depending on how many assets share identical cryptographic material.

Further, coordinating symmetric key rotation between space-based assets becomes increasingly untenable as the number of space-based assets and the systems with which they communicate increases. For instance, if each pair of satellites in a closed system of n satellites rotates a shared symmetric key every period of time, a commonly trusted source may have to transmit each satellite n unique keys. If the satellite system communicates with other systems, these systems would also require the new keys. Thus, most optimal key management protocol is likely to jointly employ symmetric and asymmetric instruments, but limit interaction in instances where asymmetric methods are utilized.

Asymmetric cryptography, where each party possesses a public-private key pair, allows two parties to exchange a shared secret in the presence of an eavesdropper. In other words, even if an adversary observes the entire interaction between two parties, inspecting all of the information exchanged, he is unable to efficiently recover the shared secret. Thus, we assume the encrypted message, often a key to be used in a more efficient algorithm, is semantically secure and computing the private key from the corresponding public key is computationally intractable. Notably, this is the same regime which enables the aforementioned digital signatures.

Before executing an asymmetric protocol, each party releases their public key for ev-

[18] *Ibid.*

eryone to observe, while maintaining the secrecy of the private key. Below is a generalized asymmetric message exchange between Alice and Bob. Here, (pk_A, sk_A) and (pk_B, sk_B) are their public-private key pairs, respectively, $Enc(\cdot)$ and $Dec(\cdot)$ are the encryption and decryption algorithms, and m is the message to be exchanged:[19]

$$\begin{array}{lcr} \textbf{Alice} & & \textbf{Bob} \\ (pk_A, sk_A), m & & (pk_B, sk_B) \\ & \xrightarrow{\quad c = Enc(pk_B, m) \quad} & \\ & & m = Dec(sk_B, c) \end{array}$$

Note, Alice must obtain pk_B, and often additional information, such as a security parameter and an acceptable set of algorithms, in order to execute the exchange. As a result, there typically involves an initial exchange of some information between parties before a secret can be exchanged. A classic asymmetric method to exchange a secret key, known as the Diffie-Hellman Key Exchange, is as follows:[20]

$$\begin{array}{lcr} \textbf{Alice} & & \textbf{Bob} \\ a \in \mathbb{Z}_p^* & \xrightarrow{\quad g^a \bmod p \quad} & \\ & \xleftarrow{\quad g^b \bmod p \quad} & b \in \mathbb{Z}_p^* \\ k = (g^b)^a \bmod p & & k = (g^a)^b \bmod p \end{array}$$

In summary, the above involves the two-way exchange of public keys in order to negotiate

[19] The depiction most closely aligns with: Rivest, R. Shamir, A. Adleman, L. “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems.” *Communications of the ACM,* vol. 21, pp. 120-126. 1978.

[20] Diffie, W. Hellman, M. “New Directions in Cryptography.” *IEEE Transactions on Information Theory,* vol. 22, pp. 644-654. 1976.

a shared secret, k, where $(g^a \bmod p, a)$ and $(g^b \bmod p, b)$ are Alice and Bob's public-private keys pairs, respectively. Notice, after the exchange they both have computed the same secret $k = g^{ab} \bmod p$. Further, note that the public keys have not been authenticated.[21] Alice and Bob may require a third party to verify each of their identifies. Alternatively, the two may store certificates, pre-issued from a third party, to verify the source of incoming messages. Moreover, Alice and Bob had to know in advance that the Diffie-Hellman exchange was to be employed. Thus, in practice, additional communication may be required in order to agree on the appropriate public keys and algorithms to utilize.

As an additional concern, the distance covered by some up-, down, and cross-link connections may increase the latency for a message to travel from source to destination, precluding the interaction required to setup some asymmetric exchanges.[22] Therefore, it may be ideal if the secret key, and an encrypted message – both of which must be authenticated – can be communicated in single transmission, removing concerns associated with interactive protocols.

Moreover, a key management protocol should also not consume a noticeable fraction of a system's allocated bandwidth and computational resources. In general, ciphertext is longer than its corresponding plaintext. Encryption must be nondeterministic to be secure, and nondeterminism requires incorporation of additional information. Assume, for contradiction, that ciphertexts are the same size as their corresponding plaintext. In this case, ciphertexts computed for the same plaintext would be identical or a single ciphertext would have to correspond to multiple plaintexts. The former is a security vulnerability,

[21] The lack of authentication leaves Alice and Bob susceptible to the same attack conducted by Eve in the previous section with regard to digital signatures.

[22] Consultative Committee on Space Data Systems. "Space Missions Key Management Systems." ch. 4.2. Nov. 2011. https://public.ccsds.org/Pubs/350x6g1.pdf.

while the latter is a correctness issue. Therefore, encryption is not surjective, instead it must be injective without the collisions that result from shorter ciphertexts. To generate the required nondeterminism, random initialization values are inserted into algorithms for encryption, while keys remain the same.[23] The result is ciphertexts which are longer than their corresponding plaintexts and change unpredictably, based on the pseudorandomness used to generate the initialization value.

Ciphertext expansion refers to the ratio of bits of ciphertext, the initialization value, and any other information required for encryption to bits of plaintext. The only encryption scheme with a ciphertext expansion equal to 1 is the one-time pad (OTP). In this system, actors, for instance, Alice and Bob, must share key k. If Alice wishes to send message m, she sends $c = k \oplus m$ to Bob. Note, the ciphertext c is the same length as the plaintext m. To decrypt, Bob computes:

$$k \oplus c = k \oplus k \oplus m = m$$

However, if Alice uses the same key for a second message m', generating $c' = k \oplus m'$, an adversary who intercepts c and c' can compute:

$$c \oplus c' = k \oplus m \oplus k \oplus m' = m \oplus m'$$

Patterns in the language used can then compromise the message and break the scheme. Hence, its name: the *one-time* pad.

The OTP is also the only information theoretically secure cryptosystem. As long as k is generated *randomly*, the entire ciphertext assumes the same nondeterminism. Assuming the randomness of k, there does not exist a better algorithm than brute force to break the OTP. Further, if an adversary begins to apply all possible values for the key, he is likely to compute a semantically sound message and possibly believe the message

[23] For nondeterminism discussion within AES and block ciphers, see *supra* note 12.

to be m. An algorithm which locates the actual key may take years or decades to halt. The drawback of the OTP rests in its lack of key reusability, creating a significant key management issue. Coordinating the use and delivery of distinct keys of size λ for every message block of size λ is often untenable.

In addition, AES with Cipher Block Chaining (AES-CBC), a widely employed block mode, has a ciphertext expansion that approaches 1 as the size of the plaintext grows. AES-CBC requires storage of a random initialization vector, but otherwise has a ciphertext expansion ratio of 1. On the other hand, Galois Counter Mode (GCM) – which encrypts the message and generates an authenticity tag – requires a single initialization value to generate a ciphertext the size of the message and a 16 byte authentication tag.[24] Thus, while the overall ciphertxt expansion of AES-GCM is larger than AES-CBC, AES-GCM provides a low-overhead means for authentication. A protocol using AES-CBC would have to find a mechanism to verify authenticity, and while MACs and HMACs can provide similar expansion compared to the AES-GCM authentication tag, MACs and HMACs will require a distinct key thereby generating an additional key management challenge. Nonetheless, after maximizing the amount of information that can be contained in a single transmission, assets must be able to connect to a network or remain within broadcast range in order exchange packets of information.

Due to large distances or random events which obstruct communication, satellites may dynamically enter and exit a field of view that enables connectivity, advancing the need for a protocol which exchanges a key and encrypts a mesasge in a single transmission.[25] Further, lacking line of sight, it may be impossible for two distant satellites to directly

[24] Viega, J., McGrew, D. “The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP).” Internet Engineering Task Force, Request for Comments: 4106. Jun. 2005.

[25] For intermittent connectivity listed as a constraint imposed on networks in outer space, see: Consultative Committee on Space Data Systems. “Space Missions Key Management Systems.” ch. 4.2. Nov. 2011. https://public.ccsds.org/Pubs/350x6g1.pdf.

communicate. Instead, the satellites may have to relay information through a trusted ground station or through another satellite in the air. In addition, if actors expect short satellite lifetimes, the topology of the network must be able to rapidly adjust to changes in composition. Thus, the most appropriate network model to consider is likely a mobile ad hoc network (MANET).

MANETs are infrastructureless networks that enable nodes to dynamically enter and exit the network, obviating the need for trusted third-party or central authority permission to enter the network; note, this does not mean that these nodes will be able to decrypt communication, it simply means they are able to receive broadcast information. The network topology allows for discontinuous monitoring by a command center and is designed for autonomous behavior and maintenance. MANETs have existing applications in mobile devices where nodes in the network may not always remain connected, as well as in military operations where stations or warfighters operate devices that are not available. In some cases, a warfighter may not want to emit detectable signals, in order to prevent adversarial traffic analysis from identifying his location, compelling him to temporarily disconnect his devices from the network. The MANET topology allows him to maintain the ability to receive data transmissions, without himself issuing observable electronic signals, and reconnect at any moment. This process may parallel satellites entering and exiting the physical boundaries where data transmission is feasible.

While MANETs deliver certain tactical advantages that fixed network topologies cannot, there exists a few primary system vulnerabilities, including the possible need for packets of data to hop between nodes and the ability for untrusted nodes to attempt to join the network. In many implementations, one must maintain a situation awareness of nodes in order to route messages to their destinations most efficiently. Without such awareness, one can broadcast may establish a protocol where each satellite which receives a message subsequently repeats the transmission. This approach could be effective, assuming each satellite is able to connect to another satellite and the network can avoid the formation of isolated subsets. However, the aforementioned method is likely exhaustive and unnecessarily cumbersome. Moreover, encryption may render cryptanalysis ineffective, but adversarial traffic analysis and direction finding may create security vulnerabilities if a malicious node joins the network.

Conclusion

In total, intermittent network connectivity, propagation delay, and an efficient use of bandwidth advances the previously mentioned feature of an appropriate key management protocol for space-based assets: namely, a single transmission could be required to exchange a key, encrypted a message, and authenticate both of the aforementioned. Space-based systems must be communicatively interoperable before protected communication is realized, but if systems are interoperable, they may additionally employ similar algorithms for confidentiality, integrity, and authenticity, as well as support compatible approaches to key management.

Nonetheless, assets which may orbit the globe in less than 90 minutes incite international concern. Mistakes in deployment can affect a range of countries and peoples, requiring guidelines that not only support use of the domain, but also promote responsible and sustainable operations in the environment. In some cases, technical solutions coupled with public policy may assist actors in adhering to, and enforcing, internationally recognized guidelines. This study now transitions to examine existing policy which governs the domain in order to later present a specific toolkit for key management which not only addresses technical concerns, but also may promote cross-constellation interoperability and consequent compliance with an existing body of international law.

3 Space as an International Domain

In addition to the aforementioned technical challenges, space-based assets operate in a domain which holds international interest, but remains plagued by political differences. Varying interpretation and enforcement of the same text may subjugate the international environment to the least prohibitive legal regime, leading to a less reliable, sustainable space environment. To augment the design of an appropriate key management protocol for outer space, this section studies the diplomatic efforts which provide a basis for the behavior of actors in the domain. The result may be a technical solution which delivers a diplomatic tool to accomplish a political objective – namely the responsible use of outer space in accordance with international law.

Outer space is increasingly contested, inviting efforts to command the domain for both commercial and military applications. Some states may act unilaterally when determined, as in any other global common, but multilateral campaigns driven by states and commercial actors could be the most effective mechanism to enforce existing international law, support the interests of stakeholders, and address the long-term sustainability of outer space. The UN is unrivaled in its attempts to promote order between international parties and across international domains. However, the commercial outer space industry presents additional challenges associated with international jurisdiction and the differences between each state's legal code. Further, the world body lacks mechanisms to enforce existing provisions related to outer space, and without statutory codification of its directives by member states, global legal frameworks may have little effect. As historian Paul Kennedy notes, "it was useless for the Netherlands to ban industrial discharges into the Rhine if the nations upriver did not,"[26] and policies for behavior in outer space have little impact absent near global adoption.

This section first assesses the international legal framework presented by the UN, with a focus on its application to outer space. Then this chapter considers the landscape of government and commercial satellite deployment, comparing the interests of stakeholders and depicting areas of overlapping services where cooperation may be amenable to both parties. Here, robust cooperation may assist nations to address international concerns related to continued supervision and debris mitigation. This section further studies the operation of undersea cables in order to illustrate an area of interoperability between commercial entities with assets in a global common governed by UN diplomacy. In the end, cooperation between satellite systems which achieve a certain degree of technical – and minimally communicative – interoperability, as observed in the submarine cable industry, may result in enhanced compliance to international concerns as a result of collective benefit from the system, rather than instruments of enforcement.

3.1 International Legal Framework

The absence of a world venue for diplomatic remediation was widely realized after the First World War. In response, states formed the League of Nations to, as written in the Treaty of Versailles (1919), "promote international [cooperation] and to achieve international peace and security."[27] Twenty-seven states agreed to the Covenant of the League of Nations at its inception, and over time the forum enjoyed several successes.[28]

[26] Kennedy, P. *The Parliament of Man: The Past, Present, and Future of the United Nations.* New York: Random House, 2006. pp. 157-158.

[27] Treaty of Versailles, part 1, Covenant of the League of Nations, preamble, Jun. 28, 1919.

[28] This total does not double count for countries within the British Empire, including Canada, Australia, South Africa, New Zealand, and India. Moreover, 13 additional states were invited to join the

The League settled border disputes, advocated for the rights of ethnic minorities, formed the International Labor Organization (ILO), and most notably, presented states with a new, more international view of the world.[29] The climate generated by the League enabled states to cooperate on international postal services, maritime agreements, air traffic control, and encouraged cultural understanding which supported the relatively halcyon period of the 1920s.[30]

The League would ultimately fracture, in part due to violent territorial disputes in the 1930s, but mostly from its limited international influence. The forum lacked representation from imperial colonies and could not sustain lasting endorsement from contemporary powers. Further, acts of aggression executed by current and former League members, including Japan's invasion of Manchuria, the Soviet Union's invasion of Finland, and Germany's invasions throughout Western Europe, deteriorated the League's legitimacy. League member states' ultimate decision not to enforce provisions within the Covenant of the League of Nations, namely Article 16 which asserts that "[s]hould any Member of the League resort to war in disregard of its covenants . . . it shall *ipso facto* be deemed to have committed an act of war against all other Members of the League," reinforced the League's tenuous international standing and led to the demise of the body.[31]

Toward the end of World War II, motivated by sentiments similar to those underlying the establishment of the League of Nations, but in further view of the League's shortcomings in adoption and enforcement, the Charter of the United Nations was signed on June 26, 1945. Today, there are 193 member states which submit one representative

agreement at its inception; *Id.*, annex.

[29] Kennedy, P. *The Parliament of Man: The Past, Present, and Future of the United Nations.* New York: Random House, 2006. pp. 10-11.

[30] *Ibid.*

[31] *Id.* at pp. 10-13; Treaty of Versailles, part 1, Covenant of the League of Nations, art. 16, Jun. 28, 1919.

to the General Assembly and collectively pursue the three objectives: the maintenance of international security; the advancement of the world economy; and the promotion of cultural understanding.[32] Ultimately, the UN retains consistent support from the world's greatest powers and sustains vast international representation, consequently providing a legitimized venue for discourse on a range of global issues, including human rights, laws of the sea, drought, and ozone depletion.[33]

Nonetheless, while UN-brokered treaties may act as national legal instruments to provide an enforcement mechanism within states, many UN directives are neither legally binding nor identically interpreted. For instance, as Paul Kennedy notes with regard to the International Covenant on Economic, Social, and Cultural Rights of 1966, signatories "knew that [the rights contained in the Covenant] were aspirations, not statutory obligations, and that different countries would respond to these proclaimed 'rights' in different ways."[34] The same is true of many provisions, such as the Universal Declaration of Human Rights, adopted by the General Assembly in 1948 to deliver men and women of all nationalities, races, and religions equal rights to free expression, government participation, education, and much more.[35] Ultimately, UN directives are as imperfect as the systems which produce them. International agreements require adhesive to stick with each signatory, and cohesion is likely to result from mutual interest coupled with effective tools to enforce the law. The same holds for any framework to guide the behavior of

[32] Objectives of UN illustrated in: Kennedy, P. *The Parliament of Man: The Past, Present, and Future of the United Nations.* New York: Random House, 2006. pp. 31-32; Up-to-date UN member list at: https://www.un.org/en/sections/about-un/overview/index.html.

[33] *Id.* at pp. 13; United Nations Convention on the Law of the Sea, Dec. 10, 1982, 1833 U.N.T.S. 397; United Nations Convention to Combat Desertification in those Countries Experiencing Serious Drought and/or Desertification, Particularly in Africa, Oct. 14, 1994, 1954 U.N.T.S. 3; United Nations, Montreal Protocol on Substances that Deplete the Ozone Layer, Sept. 16, 1996, 1522 U.N.T.S. 3.

[34] Kennedy, P. *The Parliament of Man: The Past, Present, and Future of the United Nations.* New York: Random House, 2006. pp. 184.

[35] United Nations General Assembly resolution 217 A, Universal Declaration of Human Rights, Dec. 10, 1948.

actors in outer space.

United Nations Laws of Outer Space

The United Nations General Assembly established the Committee on the Peaceful Uses of Outer Space (COPUOS) in 1959 to study the domain and anticipate the "legal problems which may arise from the exploration of outer space."[36] COPUOS consisted of 24 members at its inauguration and now contains 92 members which additionally participate in two subcommittees: the Scientific and Technical Subcommittee and the Legal Subcommittee.[37] Today, the committee remains the leading apparatus within the UN to issue scientific and legal guidelines pursuant to UN objectives in security, economic advancement, and cultural understanding as each relates to outer space.

COPUOS framed space exploration within the text of the UN Charter to issue the Declaration of Legal Principles Governing the Activities of States in the Exploration and Use of Outer Space ("Declaration of Legal Principles") for successful General Assembly adoption in 1963.[38] The Declaration of Legal Principles states that the "exploration and use of outer space shall be carried on in accordance with international law," and the provision attempts to advance cooperation by asserting that "[o]uter space and celestial bodies are not subject to national appropriation by claim of sovereignty. . . ."[39] In contrast, air space – whose upper limit is disputed but generally considered to be under the Kármán line, or 100 kilometers above sea level – is recognized as sovereign, with guidelines for international aviation services recommended by the International Civil Aviation

[36] United Nations General Assembly resolution 1472 (XIV), para. 1, Dec. 12, 1959.

[37] Up-to-date members list at: http://www.unoosa.org/oosa/en/members/index.html. Accessed: May 2019.

[38] United Nations General Assembly resolution 1962 (XVIII), Declaration of Legal Principles Governing the Activities of States in the Exploration and Use of Outer Space, Dec. 13, 1963.

[39] *Id.* at para. 3-4

Organization (ICAO), a specialized agency which works with the UN General Assembly and Economic and Social Council (ECOSOC).[40] Article I of the Convention on International Civil Aviation asserts that "[s]tates recognize that every state has complete and exclusive sovereignty over the air space above its territory."[41] In effect, COPUOS, with General Assembly endorsement, promotes outer space as a global common, leaving the domain susceptible to the same pitfalls that plague all international guidelines: presumed global adherence and lack of enforceability – rendering space like the Rhine.

In 1966, UN General Assembly, taking language from the COPUOS Legal Subcommittee, adopted the most comprehensive, widely ratified set of guidelines for international jurisprudence related to outer space. The resolution, titled the Treaty on the Principles Governing the Activities of States in the Exploration and Use of Outer Peace, including the Moon and Other Celestial Bodies ("Outer Space Treaty") transfers the ideas within Declaration of Legal Principles into a legally enforceable instrument for ratification by each member nation. Today, 109 states have ratified the Outer Space Treaty and another 23 states are signatories.[42] The document contains articles which assert that

[40] National Oceanic and Atmospheric Administration, NESDIS News and Articles. "Where is Space?" Feb. 22, 2016. https://www.nesdis.noaa.gov/content/where-space; Note, the definition of outer space is as yet undefined by the UN and may assume other altitudes, such as the lowest possible perigee of a satellite in orbit, see United Nations Committee on the Peaceful Uses of Outer Space, Legal Subcommittee, The Question of the Definition and/or Delimitation of Outer Space, A/AC.105/C.2/7, May 7, 1970; United Nations Committee on the Peaceful Uses of Outer Space, Legal Subcommittee, Definition and Delimitation of Outer Space: Views of States Members and Permanent Observers of the Committee, A/AC.105/1112/Add.2, Jan. 18, 2017; Protocol Concerning the Entry Into Force of the Agreement Between the United Nations and the International Civil Aviation Organization, annex A, May 13, 1947, 8 U.N.T.S. 315.

[41] Convention on International Civil Aviation, art. 1, Dec. 7, 1944, 61 Stat. 1180. Not all member states accede to claims of distinction between the airspace and outer space above state territory. Equatorial nations presented arguments in the Bogatá Declaration (1976) suggesting that geostationary orbit, since satellites at this altitude remain locked above their respective ground locations, should be considered sovereign territory. Constitution and Convention of the International Telecommunication Union, declarations and reservations 73, Oct. 1, 1994, 1825 U.N.T.S. 330. Geostationary orbits remain valuable positions for broadcast satellites, but the position presented in the Bogatá Declaration was not assumed by the UN.

[42] United Nations Treaty on the Principles Governing the Activities of States in the Exploration and Use of Outer Peace, including the Moon and Other Celestial Bodies, art. 7, Jan. 27, 1967, 610 U.N.T.S. 205; United Nations Committee on the Peaceful Uses of Outer Space, Legal Subcommittee, Status of International Agreements Relating to Activities in Outer Space as at January 2019, Apr. 1, 2019,

state parties agree not to "place in orbit around the earth any objects carrying nuclear weapons," provide their astronauts to "render all possible assistance to the astronauts of other States Parties" and consider requests from other states to "observe the flight of space objects."[43] All of the mentioned, along with many of the other provisions within the document, remain unlikely to be disputed or replaced in the near-term.

However, with respect to existing and near-term satellite deployment, the Outer Space Treaty contains provisions which, depending on the construction of certain terms, may easily and unavoidably be contravened. In addition, increased deployment of smaller, less physically robust assets may complicate concerns raised by COPUOS in the Outer Space Treaty. The following sections will assess each of four identified provisions within the Outer Space Treaty – Articles VI, VII, IX, and XI – that raise modern concerns regarding compliance and enforceability, but which may largely benefit from cross-constellation network interoperability.

A. Article VI

Article VI codifies approval for space-based activities and continued supervision of such activities within each ratifying state, but the extent to which states must execute either of the following remains uncertain, possibly leading to transborder differences in application of the same text and a subsequent choice of law for commercial actors with the freedom to operate from any host state. Essentially, Article VI mirrors the Declaration of Legal Principles to assert that states hold "international responsibility for national activi-

A/AC.105/C.2/2019/CRP.3.

[43] United Nations Treaty on the Principles Governing the Activities of States in the Exploration and Use of Outer Peace, including the Moon and Other Celestial Bodies, art. 4, Jan. 27, 1967, 610 U.N.T.S. 205; *Id.* at art. 5; *Id.* at art. 10.

ties in outer space, whether carried on by governmental agencies or by non-governmental entities."[44] Further, the provision writes that "non-government entities in outer space shall require authorization and continuing supervision by the [s]tate concerned."[45] In sum, the language submits that states are responsible for activities within their purview, whether performed by the state or an organization therein; further, in meeting that responsibility, states must minimally approve and supervise such activities. Ultimately, launch authorization holds clear meaning, but may present issues if approval is granted without consideration for how a state is to execute on its supervisory role.

To obtain launch authorization, some states require commercial entities to submit physical, operational, and delivery details surrounding their proposed space-based assets. For instance, satelitte operators in the U.S. must retain Federal Communications Commission (FCC) and Federal Aviation Administation (FAA) approval prior to launch. The FCC approves requests for particular frequency bands and plans for orbital debris mitigation, intending to minimize interference between space-based and terrestrial systems. The FCC also coordinates frequency allocation with the National Telecommunications and Information Administration (NTIA), which dedicates certain frequencies for federal use, and the ITU, which records internationally registered radio-frequencies.[46] Further, the FCC verifies that assets can be reasonably monitored in order to mitigate, and support the opportunity for early warning before, possible satellite collisions.[47] Regarding

[44] *Id.* at art. 6; United Nations General Assembly resolution 1962 (XVIII). Declaration of Legal Principles Governing the Activities of States in the Exploration and Use of Outer Space, para. 8, Dec. 13, 1963.

[45] United Nations Treaty on the Principles Governing the Activities of States in the Exploration and Use of Outer Peace, including the Moon and Other Celestial Bodies, art. 6, Jan. 27, 1967, 610 U.N.T.S. 205.

[46] The ITU maintains the Master International Frequency Register to inform satellite operators of frequency bands which may be available for fair use. Constitution and Convention of the International Telecommunication Union, para. 172, Oct. 1, 1994, 1825 U.N.T.S. 330.

[47] Note, Space Policy Directive-3 charges the Commerce Department to support satellite traffic monitoring and collision avoidance. Space Policy Directive-3, National Space Traffic Management Policy. Presidential Memorandum. Jun. 18, 2018. Maneuvering to avoid a collision, if supported by the spacecraft, may be performed if there exists sufficient, credible warning.

delivery and satellite retirement, 51 U.S.C. §50901 (1984) authorizes the Secretary of Transportation, utilizing the Federal Aviation Administration (FAA), "to oversee and coordinate the conduct of commercial launch and reentry operations, issue permits and commercial licenses . . . and protect the public health and safety, safety of property, and national security and foreign policy interests of the United States."[48] In effect, the FCC and FAA jointly maintain U.S. compliance with Article VI of the Outer Space Treaty.

Other states may not meet the same standards. For instance, Swarm Technologies in 2018 was denied the ability to launch four small satellites, titled the SpaceBees, from within the U.S.[49] After examining the SpaceBees' 10-by-10-by-2.5 centimeter frames and other physical specifications, the FCC asserted that the "spacecraft are . . . below the size threshold at which detection by the Space Surveillance Network can be considered routine."[50] An FCC representative wrote in the rejection letter to Swarm that "the ability of operational spacecraft to reliably assess the need for and plan effective collision avoidance maneuvers will be reduced or eliminated," provided the SpaceBees are deployed.[51] However, after FCC denial, Swarm Technologies launched its cluster from India, presenting the same risk to U.S. interests that FCC measures attempted to preclude.[52]

Even countries which seek to comply with the language of Article VI may not support consistent guidelines on how the Article's provisions may be adhered to. An investigation of the Swarm incident conducted by *IEEE Spectrum* revealed that the FCC had licensed

[48] 51 U.S.C. §50901 (b)(3). 1984.

[49] Geib. C. "The U.S. Government Has No Idea What To Do About Small Satellites." *Futurism.* Apr. 11, 2018.

[50] Federal Communications Commission, Letter to Swarm Technologies, Inc. in response to application for experimental authorization. Dec. 12, 2017. https://apps.fcc.gov/els/GetAtt.html?id=203152&x=.

[51] *Ibid.*

[52] Harris, M. "The FCC's Big Problem with Small Satellites." *IEEE Spectrum.* Apr. 10, 2018. Note, the FCC investigated the incident and Swarm Technologies later paid a $900,000 settlement. Henry, C. "FCC Fines Swarm $900,000 for Unauthorized Smallsat Launch." *Space News.* Dec. 20, 2018.

satellites with similar – and sometimes even smaller – dimensions compared to that of the SpaceBees. For example, the FCC approved the Aerospace Corporation's launch of two 5-by-5-by-10 centimeter satellites.[53] The *IEEE Spectrum* study lists a corrective comment provided by an FCC spokesperson, quoted as: "[s]ize isn't the only criteria that the FCC considers when granting experimental licenses for small satellites. Due to the number of variables to consider, the Commission takes a [holistic] case-by-case approach when granting authorizations for satellites of this size"[54] Nonetheless, the need for clarification may illustrate a degree of confusion that effects the same reality as an absence of consistent specifications, diminishing the ability to justify when abrogation of the specifications is permissible and chilling opportunities to reasonably assert claims against entities who do not enjoy such instances.[55]

In addition to dissimilar standards by which different states approve launch, there remains an Article VI challenge relating to the extent states will supervise assets and components thereof once deployed. This is likely to include monitoring each satellite's activity while the asset is functional, but Article VI does not provide insight into whether or not "supervision" should be construed to assume the monitoring of possible debris generated during deployment or regular operation of the satellite. Article VIII of the Outer Space Treaty asserts that "[o]wnership of objects launched into outer space . . . and of their component parts, is not affected by their presence in outer space,"[56] indicating that debris may be categorized as objects which require continued supervision. Although,

[53] Harris, M. "The FCC's Big Problem with Small Satellites." *IEEE Spectrum.* Apr. 10, 2018.

[54] *Ibid.*

[55] In addition, under the United Kingdom's (U.K.) Space Industry Act 2018 – which augments the Outer Space Act 1986 – the Secretary of State, or an appointed regulator, has the agency to determine how to consider debris mitigation guidelines prior to launch, possibly leading to a framework similar to the FCC's where a standard may emerge through a pattern of approvals and denials over time, without necessitating codification. United Kingdom. Space Industry Act 2018, c. 2, para. 2(h).

[56] United Nations Treaty on the Principles Governing the Activities of States in the Exploration and Use of Outer Peace, including the Moon and Other Celestial Bodies, art. 8, Jan. 27, 1967, 610 U.N.T.S. 205.

even if one constructs the language Article VI to include debris, anti-satellite (ASAT) tests, such as that conducted by India in March 2019, generate hundreds of pieces of debris that likely fall beneath the size threshold for reliable tracking, contravening even a generous interpretation of the terms.[57] In particular, countries which are eager to approve satellite launches and also generate debris through ASAT demonstrations may signal the state's interpretation of Article VI, providing daylight between such an interpretation and the application of the provision within other jurisdictions. The result may provide commercial actors a choice of law and deteriorate a global rule of law.

Moreover, while scrupulous mitigation and tracking of debris may embody responsible behavior in the domain, an unreasonable or intense burden to continually supervise activity, especially generated debris, may undercut Article I of the Outer Space Treaty which promotes the use of space by all states, "irrespective of their degree of economic or scientific development."[58] Nonetheless, the risk posed by debris has been noted by the United Nations as early as 1982, at which time the Report of the Second United Nations Conference on the Peaceful Uses of Outer Space ("UNISPACE II") claims that "[w]hile the probability of accidental collision with a 'live' space object is yet statistically small, it does exist and the continuation of present practices ensures that this probability will increase to unacceptable levels."[59] Thus, while at times contradictory, the UN may be interested in discovering methods to balance the generation of debris with encouraging states to enter the domain.

[57] In particular, NASA claims that India's anti-satellite missile test increased the likelihood that small debris would collide with the International Space Station by 44 percent over 10 days. Chappell, B. "NASA: Debris from India's Anti-Satellite Test Raised Threat to Space Station." *National Public Radio.* Apr. 2, 2019.

[58] United Nations Treaty on the Principles Governing the Activities of States in the Exploration and Use of Outer Peace, including the Moon and Other Celestial Bodies, art. 1, Jan. 27, 1967, 610 U.N.T.S. 205.

[59] United Nations, Report of the Second United Nations Conference on the Exploration and Peaceful Uses of Outer Space, Aug. 9-21, 1982, A/CONF.101/10.

Ultimately, the designation and extent of liability for activities that damage another state's assets – and perhaps culpability for a gross inability to monitor activities pursuant to the provisions – is likely to color the definitions of "international responsibility" and "supervision," noted in Article VI.[60] Thus, Article VI is more deeply examined in further view of Article VII, which attempts to cover the liability question.

B. Article VII

Article VII covers states' liability for activities in outer space, but the UN has yet to establish itself as the legitimate body to settle disputes related to outer space, likely due to a limited number of opportunities and contested definitions of terms within Article VII and its supporting instruments. The provision asserts that each state which "launches or procures the launching of an object into outer space . . . and each [s]tate . . . from whose territory or facility an object is launched, is internationally liable for damage to another [s]tate . . . its natural or juridical persons by such object or its component parts on the Earth, in air or in outer space . . . ."[61] The language submits that states are culpable for accidents related to "national activities" in outer space. However, the text lacks language which defines *how* nations are to agree on post-accident compensation, instead requesting that COPUOS "continue to work on the elaboration of an agreement on liability for damages caused by the launching of objects into outer space."[62]

In response, the COPUOS Legal Subcommittee drafted the Convention on Interna-

[60] *Supra* notes 44-45.

[61] United Nations Treaty on the Principles Governing the Activities of States in the Exploration and Use of Outer Peace, including the Moon and Other Celestial Bodies, art. 7, Jan. 27, 1967, 610 U.N.T.S. 205.

[62] United Nations General Assembly resolution 2222 (XXI), Treaty on the Principles Governing the Activities of States in the Exploration and use of Outer Space, including the Moon and Other Celestial Bodies, para. 4, Dec. 19, 1966.

tional Liability for Damage Caused by Space Objects ("Liability Convention"), which the UN General Assembly adopted in 1971.[63] Since its entry into force in 1972, 96 states have ratified the Liability Convention and 19 others stand as signatories, intending to establish procedural clarity after accidents in outer space.[64] Article I of the Liability Convention defines the terms of art to be applied later, intending to preclude future misconstruction. For instance, "launching state" is specified to cover both "a state which launches or procures the launching of a space object" and "a state from whose territory or facility a space object is launched."[65] In addition, a "space object" is constructed to include component parts of another space object, as well as the launch vehicle.[66] The resultant provision illustrates which material can cause damage – the spacecraft, its vehicle, and possibly its generated debris – and who holds liability and hence the responsibility mentioned in Article VI of the Outer Space Treaty for such objects – the launching state and, if applicable, the state with purview over the party which procured the launch.[67]

The Liability Convention further describes an apparatus to "bring about by peaceful means . . . adjustment or settlement of international disputes,"[68] as they relate to outer space, in accordance with the Charter of the United Nations. However, this system has never been directly tested; states have thus far chosen to settle disputes outside of the UN apparatus. Articles XV to XX of the Liability Convention define the Claims Commission and the process by which states are to arrive at a settlement using the aforementioned

[63] United Nations General Assembly resolution 2777 (XXVI), Nov. 29, 1971.

[64] United Nations, Convention on International Liability for Damage Caused by Space Objects, Mar. 29, 1972, 961 U.N.T.S. 187; United Nations Committee on the Peaceful Uses of Outer Space, Legal Subcommittee, Status of International Agreements Relating to Activities in Outer Space as at January 2019, Apr. 1, 2019, A/AC.105/C.2/2019/CRP.3.

[65] United Nations, Convention on International Liability for Damage Caused by Space Objects, annex art. 1, Mar. 29, 1972, 961 U.N.T.S. 187.

[66] *Ibid.*

[67] *Supra* notes 44-45.

[68] Charter of the United Nations, art. 1, Jun. 26, 1945.

body.[69] In total, the Liability Convention reinforces the obligations of states related to post-accident compensation pursuant to Articles VI and VII of the Outer Space Treaty, but the system has yet to be tested.

Even when the attribution of an accident is confirmed, parties may not view the UN as the appropriate body to settle disputes. For example, a nuclear-powered Soviet satellite, Cosmos 954, crashed in Canada, dispersing radioactive material throughout a remote area in 1978.[70] Canada spent $14 million on clean-up after the accident, but chose not to avail of the UN Claims Commission. Instead, Canada directly requested $6 million from the Soviet Union which ultimately issued only $3 million.[71]

Some argue that the Soviet Union may not have been subject to issue any indemnities, given an absence of "damage," defined in the Liability Convention as "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."[72] These claims may cut against Article V of the UN Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space ("Rescue Agreement"), entered into force in 1968, which asserts that "[e]xpenses incurred in fulfilling obligations to recover and return a space object or its component parts under paragraphs 2 and 3 of this article shall be borne by the launch-

[69] Notably, the Claims Commission is a three party committee, comprising one party that each state in the dispute selects and another party which the petitioner and respondent jointly appoint, embodying the Chairman of the Claims Commission. If parties to a dispute cannot agree on a Chairman, the Secretary-General is asked to appoint one. Further, if either the claimant or respondent do not choose a party, the Chairman comprises a one-person Claims Commissions. United Nations, Convention on International Liability for Damage Caused by Space Objects, annex art. 14-20, Mar. 29, 197, 961 U.N.T.S. 187.

[70] Cohen, Alexander F. "Cosmos 954 and the International Law of Satellite Accidents." *Yale Journal of International Law*, vol. 10, art. 7, 1984, pp. 89; Gwertzman, B. "Nuclear-Powered Soviet Satellite is Expected to Crash This Month." *New York Times.* Jan. 6, 1983.

[71] Notably, the Soviet Union claims the collision may have been the result of another collision which it was not able to attribute, adding to the difficulty in reaching an appropriate settlement. Cohen, Alexander F. "Cosmos 954 and the International Law of Satellite Accidents." *Yale Journal of International Law*, vol. 10, art. 7, 1984, pp. 89.

[72] *Ibid.*; United Nations, Convention on International Liability for Damage Caused by Space Objects, Annex art. 1, Mar. 29, 1972, 961 U.N.T.S. 187.

ing authority."[73] However, the referenced paragraphs 2-3 which refer to the collection of space objects within another state's jurisdiction, use the caveat "upon the request of the launching authority" preceding any action.[74] At any rate, there remains room for states to contest the definition of "damage," possibly at the expense of a functioning legal environment.

In other cases, "damage" caused by space objects is clearly sustained, yet parties choose to negotiate outside of the UN and without the Claims Commission codified in the Liability Convention. For instance, after the Iridium 33 and Russian Cosmos 2251 satellites collided in 2009, the parties settled without any UN involvement.[75] The Liability Convention does not explicitly draw standards for indemnification, but the parties – despite Iridium's status as a non-government entity based in the U.S. – settled independently. This may suggest that the parties could not reasonably blame one another; however, Cosmos 2251 was inactive while Iridium 33 was operational, indicating that Cosmos could be culpable for a deficient retirement plan.[76] Alternatively, the parties could have reached mutually agreeable terms and obviated the Claims Commission; although, this justification likely does not scale to other incidents – such as Canada's choice to avoid UN arbitration after the Cosmos 954 incident despite a disagreeable outcome.[77]

If a Claims Commission was assembled to arbitrate the Iridium 33 - Cosmos 2251 collision, the UN could have gained an opportunity to establish precedent – or at least foment

[73] United Nations, Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space, art. 5, para. 5, Apr. 22, 1968, 672 U.N.T.S. 119.

[74] The full language for paragraphs 2 and 3 are the following: [2] "Each Contracting Party having jurisdiction over the territory on which a space object or its component parts has been discovered shall, upon the request of the launching authority and with assistance from that authority if requested, take such steps as it finds practicable to recover the object or component parts;" [3] "Upon request of the launching authority, objects launched into outer space or their component parts found beyond the territorial limits of the launching authority shall be returned to or held at the disposal of representatives of the launching authority, which shall, upon request, furnish identifying data prior to their return." *Ibid.*

[75] Weeden, B. "2009 Iridium-Cosmos Collision Fact Sheet." *Secure World Foundation.* Nov. 10, 2010.

[76] *Ibid.*

[77] *Supra* notes 70-71.

wide disagreement to inspire further discourse – regarding the definition of "launching state" pursuant to the Liability Convention and continued "supervision" under Article VI of the Outer Space Treaty.[78] For instance, Iridium 33 was launched from Kazakhstan on a Russian launch vehicle, and the Claims Commission would have determined whether the "launching state," comprises U.S., Russia, Kazakhstan, or some combination of thereof.[79] Moreover, a collision warning was not issued by either the U.S. or Russia. Thus, a Claims Commission may have apportioned liability based on grounds that both any combination of the "launching states" may have had a responsibility to monitor their respective satellites.[80] Depending on the ruling, it could have indicated if Article VI of the Outer Space Treaty constructs "supervision" of activities to cover the monitoring or tracking of inactive satellites and other debris.[81]

Further, assuming the provenance of space objects can be attributed, the fractional apportionment of liability in cases which may result from an initial collision has yet to be tested. Article IV of the Liability Convention declares state parties to the launch are "jointly and severally" liable, and indemnities "shall be apportioned between the... [s]tates in accordance with the extent to which they were at fault."[82] For instance, after China demonstrated an ASAT missile in 2007, resultant debris in orbit may have collided with a Russian satellite in 2013.[83] Russia did not pursue legal action against China, likely

[78] United Nations, Convention on International Liability for Damage Caused by Space Objects, art. 1, Mar. 29, 1972, 961 U.N.T.S. 187; United Nations Treaty on the Principles Governing the Activities of States in the Exploration and Use of Outer Peace, including the Moon and Other Celestial Bodies, art. 7, Jan. 27, 1967, 610 U.N.T.S. 205.

[79] Launch vehicle and state of launch, see: Weeden, B. "2009 Iridium-Cosmos Collision Fact Sheet." *Secure World Foundation.* Nov. 10, 2010; The Liability Convention defines "launching state" as both a "[s]tate which launches or procures the launching of a space object" and a"[s]tate from whose territory or facility a space object is launched. United Nations, Convention on International Liability for Damage Caused by Space Objects, art. 1, Mar. 29, 1972, 961 U.N.T.S. 187.

[80] *Supra* notes 75-76.

[81] *Supra* note 45.

[82] United Nations, Convention on International Liability for Damage Caused by Space Objects, art. 4, Mar. 29, 1972, 961 U.N.T.S. 187.

[83] Tate, K. "Russian Satellite Crash with Chinese ASAT Debris Explained." *Space.com.* Mar. 8, 2013.

due to the low value of the damaged satellite, the burden to prove that the debris in fact resulted from the ASAT test, and the politics involved with such a dispute.[84] However, assuming the aforementioned collision occurred, it remains to be determined if China now assumes the responsibility to supervise debris ejected from the Russian satellite under Article VI and the liability attached to any future collisions associated with such debris under Article VII.

In the end, the UN framework for supervision in Article VI and liability in Article VII of the Outer Space Treaty, with the support of the Liability Convention, has not received rigorous testing. Nevertheless, as outer space becomes more congested, the frequency of disputes is likely to rise, resulting in the instantiation of UN Claims Commissions. However, as increasing debris accumulation makes attribution more doubtful, an international sustainability plan and an agreement for responsible use of the domain is probably the most effective mechanism for actors to protect their assets. Articles IX and XI provide the foundation for any such approach.

C. Article IX

In recognizing space as global domain where activities may result in cross-national effects despite the responsibilities and potential liabilities assigned by Article VI and VII, Article IX of the Outer Space Treaty provides states an opportunity to preempt activities which may jeopardize existing assets or impede future use of the domain. Article IX asserts two primary principles. First, State Parties shall avoid "harmful contamination and also adverse changes in the environment . . . resulting from the introduction of

[84] David, L. "Legal Action Against China Unlikely in Orbital Debris Collision." *Space News.* Mar. 13, 2013.

extraterrestrial matter . . . ."[85] Second, if a "State Party to the Treaty which has reason to believe that an activity or experiment planned by another State Party in outer space . . . would cause potentially harmful interference with activities in the peaceful exploration and use of outer space . . . [the State Party] may request consultation concerning the activity or experiment."[86]

To comply with the first Article IX principle, and prevent the need to respond to the second, states may collectively minimize contamination – as well as reduce the likelihood of collisions – through efforts to limit debris resulting from the deployment, retirement, and continued operation of spacecraft. NASA and ESA participated in the first internationally coordinated orbital debris mitigation effort in 1987, responding to the 1986 explosion of Airane I in low earth orbit.[87] By 1993, this effort grew to form the Inter-Agency Space Debris Coordination Committee (IADC) which today has 13 member agencies which cooperate on debris research and mitigation.[88] On the world stage, the Scientific and Technical Subcommittee of COPUOS in 1994 addressed space debris for the first time within the UN, stating the need to develop "appropriate and affordable strategies to minimize the potential impact of space debris on future space missions."[89]

In total, debris mitigation programs are presented in international forums and sometimes entered into law within states, but absent near global adoption and meaningful standards, such efforts may mean little to mitigate the likelihood of collisions and sustain a reliable environment. For instance, in 2007 the UN General Assembly endorsed

[85] United Nations Treaty on the Principles Governing the Activities of States in the Exploration and Use of Outer Peace, including the Moon and Other Celestial Bodies, art. 9, Jan. 27, 1967, 610 U.N.T.S. 205.

[86] *Ibid.*

[87] Johnson, Nicholas. "Origin of the Inter-Agency Space Debris Coordination Committee." NASA Technical Reports Server. doc. id: 20150003818, Apr. 1, 2015.

[88] For members, see: https://www.iadc-online.org/. Accessed: May 2019

[89] United Nations Committee on the Peaceful Uses of Outer Space, Report of the Scientific and Technical Subcommittee on the Work of its Thirty-First Session, A/AC.105/571, p. 64, Mar. 10, 1994.

COPUOS guidelines, built from those of the IADC, which promote seven measures to broadly prevent in-orbit breakage, remove retired spacecraft from densely populated orbital regions, and limit the debris released for normal operation.[90] The IADC supports similar language, but notably recommends actors "limit[] the objects released during normal activity," choosing to use the term *objects* over *debris* and possibly indicating the UN takes more generous approach to the presence of objects in orbit.[91] In fact, COPUOS agreed that UN Space Debris Mitigation Guidelines would "not be more stringent than IADC guidelines," likely to allow states with emerging space activities first to join the domain, and then perhaps to consider IADC provisions.[92] However, the UN Assembly also submits the guidelines are non-instrumental, "remain[ing] voluntary and not [to] be legally binding under international law."[93]

To enforce IADC and UN guidelines, some states produce their own debris mitigation programs. As mentioned with regard to Article VI and pre-launch approval, the FCC interprets its statutory authority for governing radio services and satellite communication to extend to the mitigation of orbital debris.[94] As a result, actors wishing to deploy space-based systems must submit a plan to the FCC which addresses each of the following: "control of debris during normal operations;" minimization of "debris generated by

[90] United Nations General Assembly report, Space Debris Mitigation Guidelines of the Committee on the Peaceful Uses of Outer Space, annex 4, A/AC.105/890, Mar. 6, 2007; The seven guidelines, as written by COPUOS are as follows: 1) "Limit debris released during normal operations;" 2) "Minimize the potential for breakups during operational phases;" 3) "Limit the probability of accidental collision in orbit;" 4) "Avoid intentional destruction and other harmful activities;" 5) "Minimize potential for post-mission break-ups resulting from stored energy;" 6) "Limit the long-term presence of spacecraft and launch vehicle orbital stages in the low-Earth orbit (LEO) region after the end of their mission;" and 7) "Limit the long-term interference of spacecraft and launch vehicle orbital stages with the geosynchronous Earth orbit (GEO) region after the end of their mission." *Id.*

[91] Inter-Agency Space Debris Coordination Committee. "IADC Space Debris Mitigation Guidelines." Sept. 2007.

[92] United Nations General Assembly report, Space Debris Mitigation Guidelines of the Committee on the Peaceful Uses of Outer Space, para. 92, A/AC.105/890, Mar. 6, 2007

[93] *Ibid.*

[94] Federal Communications Commission Report and Order, "Mitigation of Orbital Debris." Jun. 9, 2004. 19 FCC Rcd 11567 (14).

accidental explosions;" "selection of a safe flight profile and operational configuration;" and "post-mission disposal of space structures."[95] In addition, the UN produces a Compendium on the Space Debris Mitigation Standards Adopted by States and International Organizations which collects the national mechanisms, or lack thereof, employed by at least 30 states.[96] Where instantiated, these guidelines are compulsory, but not without flaw.

States may additionally comply with Article IX through enhanced situational awareness, monitoring objects in orbit to prevent collisions and the subsequent release of debris. Although, the ability to detect collisions is often limited, as is the ability to relocate some satellites which may sustain impact. For example, the U.S. Department of Defense's Joint Space Operations Center (JSpOC) tracks over 40,000 human-made objects in orbit; however, millions more are too small to track and catalog.[97] Further, a 2017 ESA report indicates that only 15-20% of payloads in low Earth orbit (LEO) attempt to execute debris mitigation measures, and only 5% of all payloads do so successfully.[98] Thus, assuming challenges in situational awareness and satellite immobility remain, the most effective option to decrease the likelihood of collisions and the amount of debris generated, as well as closely adhere to Articles VI, VII, and IX, may be to limit the number of objects in space.[99]

[95] *Id.* at para. 2.

[96] United Nations Committee on the Peaceful Uses of Outer Space, Compendium of Space Debris Mitigation Standards Adopted by States and International Organizations, Feb. 25, 2019.

[97] Phillips, V. (editor) "Assessing Object Population in Earth Orbit." NASA publication. Last update: Aug. 7, 2017. https://www.nasa.gov/feature/assessing-object-population-in-earth-orbit.

[98] European Space Agency, Space Debris Office. "ESA's Annual Space Environment Report." May, 18, 2018. The same report suggests that by the end of 2017, at least 489 fragmentation events, or incidents where a spacecraft breaks-up in orbit due to adverse aerodynamics, collisions, anti-satellite missiles, or other anomalous reasons, will have occurred. *Id.*

[99] Satellite operators have incentive to install in orbit maneuvering capabilities on their buses, but the function may consume more resources than it is worth. On high value assets, such as the International Space Station (ISS) and those critical to national security, this ability is imperative. For instance, the ISS from 1999 to 2018 conducted 25 evasive maneuvers. Liou, J.C.. "U.S. Space Debris Environment, Operations, and Research Updates." NASA presentation to the Scientific and Technical Subcommittee on the Peaceful Uses of Outer Space, United Nations. Jan. 29 - Feb. 9, 2018. However, with respect

Article IX also asserts that a state "which has reason to believe that an activity or experiment planned by another [s]tate . . . would cause potentially harmful interference with activities in the peaceful exploration and use of outer space . . . may request consultation concerning the activity or experiment."[100] In effect, a state may accuse another state with negligence if the latter does not demonstrate reasonable efforts to mitigate the debris associated with assets under its purview. Granted, without a demonstrable injury, it may be difficult to form a compelling case. However, in addition to concerns regarding space-based assets, states may also have the liberty to voice concerns regarding activities in outer space which pose a risk to existing ground-, sea-, and air-based systems.

For example, commercial entities plan to coat the globe with broadband, but the number of assets required and the expected lifetimes of such assets may present credible risks to terrestrial activities. For instance, SpaceX in November 2018 received FCC approval to launch an approximately 12,000 satellite constellation, titled Starlink, no later than November 19, 2027. However, an *IEEE* study concludes that this constellation alone will cause an extra 500,000 objects to collide with Earth every six years.[101] The same study asserts that once Starlink is deployed, there is 45% likelihood that debris

to commercial actors conscious of size, weight, power, and cost, maneuvering may be a luxury, and its absence a risk worth taking. Moreover, states may not have the authority or ability to relocate objects in orbit if a space situational awareness service determines that an accident is likely to occur. This practice provides satellite operators additional freedom, but may simultaneously threaten assets critical to national security, public safety, and the global economy, challenging the FAA's ability to adhere to its statutory obligation to protect such assets. *Supra* note 48. Congressional leaders have proposed competing bills to deliver either the Commerce Department, in coordination with NASA, or the FAA, under the Department of Transportation, the responsibility to manage traffic in outer space. There remains disagreement within the legislative branch as to which apparatus is more postured to handle the mission. Foust, Jeff. "House Science Committee Approves Space Traffic Management Bill." *Space News.* Jun. 27, 2018; Foust, Jeff. "Senate Introduces Bill to Streamline Commercial Space Regulations." *Space News.* Jul. 27, 2018.

[100] United Nations Treaty on the Principles Governing the Activities of States in the Exploration and Use of Outer Peace, including the Moon and Other Celestial Bodies, art. 9, Jan. 27, 1967, 610 U.N.T.S. 205.

[101] Harris, M. "Here are the Odds That One of SpaceX's Internet Satellites Will Hit Someone." *IEEE Spectrum.* Dec. 17, 2018. Kepler Communications, Telesat Canada, and LeoSat received similar approval for the deployment of constellations of small satellites in low earth orbit. Caleb, H. "FCC Aproves SpaceX, Telesat, LeoSat, and Kepler Internet Constellations." *Space News.* Nov. 15, 2018.

associated with constellation will cause an injury or death every six years.[102]

Ultimately, it may be difficult to preemptively charge a state with negligence, and risks are assumed with every constellation's deployment, but the risks compound as additional actors deploy similar assets. Thus, adequate compliance with Article IX may entail reasonable efforts to limit the number of assets required to deliver a service – as the IADC recommends and the UN guidelines choose not to endorse. Article XI is a step in that direction.

D. Article XI

Article XI requires UN registration of space objects, possibly increasing the likelihood of attribution after an accident and preventing actors from submitting objects to similar orbits, but states and commercial entities additionally benefit from registration with functional agencies, such as the ITU, which require detailed information with a narrow focus. Prior to the Outer Space Treaty, the UN General Assembly adopted resolution 1721 B (XVI) in 1961 to request that "the Secretary-General maintain a public registry" of objects launched "into orbit or beyond" in order to promote cooperation across actors in outer space.[103] To elevate the registry into law, Article XI of the Outer Space Treaty asserts that states "agree to inform the Secretary-General of the United Nations as well as the public and the international scientific community, to the greatest extent feasible

[102] NASA publishes toolkits, such as the Object Reentry Survival Analysis Tool (ORSAT), to assist commercial entities in identifying the risks associated with their spacecraft before seeking FAA approval. NASA, Astromaterials Research & Exploration Science, Orbital Debris Program Office. "ORSAT." https://orbitaldebris.jsc.nasa.gov/reentry/orsat.html. Further, NASA states that there should be less than a 1 in 10,000 chance that debris do not successful dissolve on descent. While SpaceX has demonstrated a probability of roughly 1 in 17,400 of unsuccessful incineration – which is the highest among likelihoods for each of the vehicles and altitudes – but the sheer size of the constellation makes the expectation non-negligible. Harris, M. "Here Are the Odds That One of SpaceX's Internet Satellites Will Hit Someone." *IEEE Spectrum.* Dec. 7, 2018.

[103] United Nations General Assembly resolution 1721 B (XVI), para. 1-2, Dec. 20, 1961.

and practicable, of the nature, conduct, locations and results" of its activities in outer space.[104] In doing so, the Secretary-General publicly discloses the information in line with the core principles of the UN Charter – security, economic advancement, and cultural understanding.[105]

Upon initial ratification, the Outer Space Treaty contained limited specifics regarding the maintenance of an international registry and the information to be contained therein. Later, the General Assembly in 1974 adopted resolution 3235 (XXIX), containing the COPUOS Legal Subcommittee's Convention on the Registration of Objects Launched into Outer Space ("Registration Convention"), which later entered into force in 1976.[106] The Registration Convention directs the Secretary-General to compile an international registry, as described in the Outer Space Treaty, and requires each state to maintain a separate database of its respective space objects.[107] Today, 69 states have ratified the Registration Convention, and the UN maintains an active online database of internationally registered space objects, which the UN Office of Outer Space Affairs (UNOOSA) asserts, as of May 2019, to contain "89% of all satellites, probes, landers, crewed spacecraft and space station flight elements launched into Earth orbit or beyond."[108]

[104] United Nations Treaty on the Principles Governing the Activities of States in the Exploration and Use of Outer Peace, including the Moon and Other Celestial Bodies, art. 11, Jan. 27, 1967, 610 U.N.T.S. 205.

[105] *Supra* note 32.

[106] United Nations General Assembly resolution 3235 (XXIX), Jan. 14, 1975; United Nations Convention on the Registration of Objects Launched into Outer Space, Sept. 15, 1976, 1023 U.N.T.S. 15.

[107] *Id.* at art. 2-3.

[108] United Nations, Office of Outer Space Affairs. "United Nations Register of Objects Launched into Outer Space." Accessed: May 2019. http://www.unoosa.org/oosa/en/spaceobjectregister/index.html; A university study assessing the UNOOSA catalog concludes that from October 1957 to December 2014, 94.6% of payloads were registered with the UN. Jakhu, R., Jasani, B., McDowell, J. "Critical issues Related to Registration of Space Objects and Transparency of Space Activities." *Acta Astronautica.* vol 145, pp. 406-420. 2018. This may suggest any combination of the following: certain space assets mentioned above are unlikely to be registered with the UN; states may still register objects launched since December 2014; UNOOSA has identified more space objects than the university study; or the willingness of states and international organizations to register space objects with the UN has decreased. The difference remains unclear, but the aforementioned university study concludes that if the date range is extended to July 2017, only 92% of payloads have been registered, which the study attributes to a typical pattern of delay in state registration. *Id.*

Notably, there appears to be consistency in the information submitted to the UN on behalf of space launching states. The Registration Convention establishes a minimum amount of information which must be provided for launches which each state chooses to submit, likely establishing a bar for all national instruments which require registration.[109] For instance, in the U.S., 14 CFR §417.19 begins with: "[t]o assist the U.S. Government in implementing Article IV of the 1975 Convention on Registration of Objects Launched into Outer Space . . . ."[110] The section later requires that private operators of space objects and launches must submit exactly the information required by the Registration Convention to the FAA.[111] Notably, 14 CFR §417.19 provides an exception for objects owned or operated by the U.S. government, possibly because certain assets do not fall under the purview of the Department of Transportation, but consequently precluding the existence of a comprehensive registry.[112]

Even so, it remains unclear how much benefit would be obtained if all satellites were registered in the fashion dictated by the UN. In some cases, the definition of "launching state" provided in the Registration Convention results in the same complications associ-

[109] Pursuant to Article IV of the Registration Convention, the UN registry must include the date of launch, launching territory, and orbital information including period, inclination, apogee, and perigee. United Nations Convention on the Registration of Objects Launched into Outer Space, art. 4, Sept. 15, 1976, 1023 U.N.T.S. 15.

[110] 14 CFR §417.19 2011.

[111] *Supra* note 109. The only distinction is that 14 CFR §417.19 does not require specification of a launching state or states. *Id.*

[112] It is interesting to note the information provided with respect to the "[g]eneral function of the space object" specified by the Registration Convention and 14 CFR §417.19 (2011) is consistent, but fairly limited. United Nations, Convention on the Registration of Objects Launched into Outer Space, art. 4, Sept. 15, 1976, 1023 U.N.T.S. 15. For instance, the U.S. report to the UN pursuant to the Registration Convention spanning launches from January to April 2017 lists 121 space objects, 118 of which are listed with the general purpose of: "[s]pacecraft engaged in practical applications and uses of space technology such as weather or communications." United Nations, Note verbale dated 1 June 2017 from the Permanent Mission of the United States of America to the United Nations (Vienna) addressed to the Secretary-General, ST/SG/SER.E/803, distr. Dec. 27, 2017. Note, this is the most recent report distributed by the UN database with respect to U.S. launches. It is unclear how much benefit a more detailed description would deliver to the international community, and such an assessment requires additional examination. However, the existing policy appears to balance the registration of space objects with each state's possible national security interests.

ated with term construction in the Liability Convention.[113] Ultimately, commercial space object approval and registration within each state is dictated jointly by Articles VI and XII, with support from Article VII, but the impact of the roughly 10% of satellites in orbit not registered with the Secretary-General, according to UNOOSA, remains uncertain, especially as accessible means for satellite tracking become more sophisticated and may afford actors the same information as UN registration.

Thus, simple registration of satellites and launches may not necessarily benefit actors in outer space, but registration with certain functional agencies within the UN – even if not explicitly required by Article XI of the Outer Space Treaty or the Registration Convention – may provide noticeable benefit to all actors. For example, the ITU records transmission wavelengths for distinct satellite systems, as well as orbital positions for satellites in geo-stationary orbit.[114] The Constitution of ITU has been ratified by all 193 UN member states, nearly 100 more ratifications than the Liability Convention and 84 more than the Outer Space Treaty itself.[115] Granted, the ITU provides functions relevant to other sectors besides satellite operation, such as issuing recommendations for ground-based radio-communications systems and assisting developing countries in the establishment of information services. However, united acceptance of the ITU is likely a product of unanimous acknowledgment of its limited, but clear role in protecting

[113] The Registration Convention defines "launching state" to mean a "[s]tate which launches or procures the launching of a space object" and a "[s]tate from whose territory or facility a space object is launched." United Nations, Convention on the Registration of Objects Launched into Outer Space, art. 1, Sept. 15, 1976, 1023 U.N.T.S. 15. See *supra* note 66 and associated text for language in the Liability Convention. Further, "space object" is defined to include "component parts of a space object as well as its launch vehicle and parts thereof." *Ibid.* For examples of complications in space object registration, see INTELSAT and INMARSAT discussion in Jakhu, R., Jasani, B., McDowell, J. "Critical issues Related to Registration of Space Objects and Transparency of Space Activities." *Acta Astronautica.* vol 145, pp 406-420. 2018.

[114] Constitution and Convention of the International Telecommunication Union, para. 11-12, Oct. 1, 1994, 1825 U.N.T.S. 330.

[115] United Nations Committee on the Peaceful Uses of Outer Space, Legal Subcommittee, Status of International Agreements Relating to Activities in Outer Space as at January 2019, Apr. 1, 2019, A/AC.105/C.2/2019/CRP.3.

international services – a feature which may be the hallmark of well-regarded registration systems.

Conclusion

The Outer Space Treaty constitutes the most comprehensive international legal framework to advance the objectives within the UN Charter as they relate to outer space. With support from the Liability Convention and Registration Convention, the framework awaits rigorous testing from modern satellite deployment, and may possibly require adjustment in view of changing political and operational dynamics within the domain.[116] Existing language may require further construction, such as the terms "supervision," "launching state," and "damage."[117] Moreover, once agreed upon, if an overwhelming number of states consistently enforce the provisions through legal instruments within their jurisdictions, the provisions may sustain lasting legitimacy and promote operational sustainability.

Even with additional detail to the existing legal framework, outer space may congest at an unnecessary pace, depriving various altitudes of future usability. As satellites become more ubiquitous, interoperability with other systems can prove to be advantageous

[116] There are other UN treaties and resolutions which attempt to address issues related to outer space, but are not as applicable to satellite deployment as the agreements mentioned in the previous section. For instance, the Rescue Agreement. See *supra* note 73. Although, the Agreement Governing the Activities of States on the Moon and Other Celestial Bodies ("Moon Agreement"), which has only been ratified by 18 member nations, may provide insight into what countries are not willing to accede to in outer space. United Nations Committee on the Peaceful Uses of Outer Space, Legal Subcommittee, Status of International Agreements Relating to Activities in Outer Space as at January 2019, Apr. 1, 2019, A/AC.105/C.2/2019/CRP.3. The Moon Agreement asserts that states will, among other things, not contest the moon from a military (Article III) and commercial perspective (Article XI). United Nations, Agreement Governing the Activities of States on the Moon and Other Celestial Bodies, Dec. 5, 1979, 1363 U.N.T.S. 3. The U.S.likely did not ratify the Moon Agreement because the provisions limit the freedom of commercial entities to monetize the moon's resources and deliver other countries increased political control of the forum. Griffin, N. "Americans and the Moon Treaty." *Journal of Air Law and Commerce*, vol. 46, art. 6, pp. 750. 1981.

[117] *Supra* notes 44, 65, 72.

for all parties. Effective cooperation could maximize service availability and decrease the cost to deploy certain services. Moreover, the result may enhance compliance with Article IX and minimize risk under Articles VI and VII of the Outer Space Treaty. To understand the interests of state and non-state actors, and assess the extent to which satellite system interoperability may be feasible, this study next depicts the existing and near-term landscape of space-based systems.

3.2 Modern Asset Deployment

While some satellite constellations are likely to operate in isolation, opportunities consistently increase for actors to leverage the services of one another. Moreover, even in areas where satellite systems may remain distinct, their independent services may still be utilized for a single objective, provided adequate information security which meets the demands of the service. This section first discusses areas where space-based systems are likely to remain distinct, based on two primary points: mission-specific equipment and resource allocation; and differences in information security standards. This section then illustrates that with sufficient consideration for the operational modalities of existing constellations, cross-constellation cooperation between distinct satellite operators may not only reduce costs and increase service resiliency, but also assist with compliance pursuant to the aforementioned legal framework.

First, satellites which support defense operations often retain equipment tailored for a particular objective, requiring constant mission focus and precluding features of interoperability with other systems. For instance, the U.S. Air Force deployed 23 satellites from 1970 to 2007 as part of the Defense Support Program (DSP) which intends to deliver real-time missile tracking. The buses can contain up to 6,000 detectors and infrared sensors to search for heat information ejected by missile boosters.[118] In addition, the U.S. Missile Defense Agency (MDA) operates the Satellite Tracking and Surveillance System (STSS) to, along with DSP assets, provide active missile trajectory information for ballistic missile defense systems, such as the Terminal High Altitude Area Defense (THADD) system.[119] Like DSP, STSS buses contain dedicated equipment to refine their coverage on spatially changing objects with narrowly focused sensors and to transmit the collected information to on-board signal processing tools tailored for a given objective.[120] The specifics aside, these systems require uninterrupted service over regions of choice and specialized on-board resources tailored to a particular objective, likely precluding the use of other constellations to reduce costs and enhance service resiliency at an equivalent fidelity.

Second, some constellations may have information security requirements which do not encumber other space-based assets, leaving systems with high degrees of security to operate in isolation. For instance, the U.S. Department of Defense (DOD) operates AFSATCOM transponders on various satellite systems, including the Defense Satellite Communications System (DSCS) and FLTSATCOM constellations, to support military command and control.[121] The transponders likely meet dedicated DOD requirements

[118] U.S. Air Force Fact Sheet. "Defense Support Program Satellites." Nov. 23, 2015. https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104611/defense-support-program-satellites/.

[119] The future of the MDA constellation remains undecided. Plans for a next generation Precision Tracking Space System (PTSS) were scuttled by the FY2014 budget, and the two deployed STSS buses were launched 2009 with an expected operational lifetime of only two years. Missile Defense Project, "Space Tracking and Surveillance System (STSS)," *Missile Threat,* Center for Strategic and International Studies, August 11, 2016, last modified: Jun. 15, 2018, https://missilethreat.csis.org/defsys/stss/.

[120] *Ibid.*

[121] Carter, A., Steinbruner, J., Zraket, C. *Managing Nuclear Operations.* Washington, D.C.: The Brookings Institution, 1987. pp. 687. In addition, DSCS satellites operate at geosynchronous orbit, likely increasing the difficulty in disrupting or destroying each satellite with counterspace efforts, but introducing transmission delays which commercial entities may find unacceptable. U.S. Air Force Fact Sheet. "Defense Satellite Communications System." March 2003. http://www.au.af.mil/au/awc/space/factsheets/dscs.htm.

and offer a closed system for exclusively authorized personal to utilize. The result is a communication layer which may protect against adversarial direction finding, traffic analysis, and cryptanalysis, while also providing additional command over bandwidth allocation. Thus, some actors are likely to command assets with specialized equipment, dedicated objectives, and enhanced information security requirements that inherently limit the viability of robust cooperation.

Even dual, civilian and military, systems which could greatly benefit from robust interoperability may be confined to isolation due to security concerns. For example, government operated Global Navigation Satellite Systems (GNSS), such as the U.S. Global Positioning System (GPS), provide armed forces and civilians with constant position, navigation, and timing (PNT); a service that the U.S. Department of Homeland Security asserts is necessary for 14 of 16 critical infrastructure sectors.[122] Today, GPS is likely essential for defense systems which require high-degrees of in theater fidelity, such as blue-force tracking, unmanned aerial vehicles, and precision guided munitions; in addition to the role of accurate PNT in commerce, emergency services, air traffic control, and other civilian and commercial sectors. However, despite utilization of the same assets, commercial and military PNT are not equivalent.

For example, GPS satellites simultaneously broadcast encrypted packets for military position triangulation and unencrypted information for civilians to compute the same.[123] Encryption limits an adversary's ability to forge the GPS signal, but since GNSS satellites rarely receive data from the ground – providing an autonomous behavior critical to

[122] Tullis, P. "The World Economy Runs on GPS. It Needs a Backup Plan." *Bloomberg.* Jul. 25, 2018.

[123] Psiaki, M., Humphreys, T. "Protecting GPS From Spoofers Is Critical to the Future of Navigation." *IEEE Spectrum.* Jul. 29, 2016. Along with the U.S. GPS, other GNSS include Russia's GLONASS, the European Union's (EU) Galileo, and China's BeiDou constellations. In addition, systems such as the Indian Regional Navigation Satellite System (IRNSS) provide the same geolocational service for smaller surface areas.

maintaining command and control during a conflict – unique key distribution to distinct devices is impractical.

Moreover, signals from GNSS transmitters are relatively weak and can be easily spoofed. For example, a spoofing device designed by university researchers was used to redirect a yacht from its intended destination in Monaco to Greece.[124] While civilian devices can receive the signal as ciphertext, the layer of encryption hides the source satellite's unique identifier and locational information, rendering GPS devices without the correct cryptographic key unable to use the signal for position triangulation. To exacerbate the issue, university researchers found that 95% of civilian drivers will follow GPS directions along an incorrect route, indicating either that drivers believe GPS delivers the most optimal routes or that drivers would be totally lost without the technology.[125]

Note, distributing the same key to every public device renders encryption pointless, and delivering a unique key to each device requires tremendous overhead. Asymmetric forms of key exchange may be possible, but each device would have to transmit to, and exchange a key with, every GPS satellite with which it encounters – a capability that existing systems likely do not support. Further, the latency associated with this type of key exchange may be untenable for real-time service. In summary, even while some space-based systems have significant commercial impact, governments will likely maintain any dual-use space-based assets which raise concerns with national security, public safety, and the world economy – and may even slightly modify the services, as in the case with encryption and GPS, to provide a defensive advantage.

Nonetheless, with consistent equipment and security requirements across constellations, actors can utilize their relative distinctions to support the services of one another.

[124] *Ibid.*

[125] Zeng, C. et al. "All your GPS Are Belong to Us: Towards Stealthy Manipulation of Road Navigation Systems." *Proceedings of the 27th USENIX Security Symposium.* Aug. 15-17, 2018.

Further, the decline in cost to launch, miniaturization of satellites, and increased incorporation of commercial-off-the-shelf (COTS) components decreases procurement expenses and facilitates a growing market for commercial actors, suggesting that without physical and network interoperability, outer space may congest with incompatible systems at an increased, possibly irreversible pace.

Decreasing costs to launch allows commercial actors to enter the domain with unprecedented financial ease. Consider the United Launch Alliance (ULA) – a Lockheed Martin and Boeing conglomerate – which used to be the exclusive launch services provider based in the U.S.. In 2018, the U.S. Air Force included in its budget the "unit cost" for a single ULA rocket for fiscal year 2021, which amounts to $424 million.[126] Previously, the tremendous cost of ULA vehicles prevented many commercial entities from enjoying the service.[127] However, SpaceX now offers its Falcon 9 rocket for $54 million, Rocket Lab's Electron Rocket can carry small satellites to orbit for roughly $4.9 million, and Vector's rockets can deliver small packages for around $3 million.[128] Furthermore, if the cost to construct satellites themselves decreases in parallel, the number of actors with the capital to deploy assets to orbit may increase dramatically.

COTS components reduce procurement costs, and may generate separate markets for satellite manufacturing and payload construction, but may also decrease the lifetime of space-based assets. Without expensive radiation-hardened electronics, systems become

[126] Berger, E. "Air Force Budget Reveals How Much SpaceX Undercuts Launch Prices." *Ars Technica.* Jun. 15, 2017.

[127] In this case, the financial burden is likely inflated because the U.S. Air Force contracts ULA to maintain launch readiness, requiring added financial support from the Air Force. Nonetheless, launch prices typically have a high minimum, largely due to degradation of the spacecraft after a single flight.

[128] SpaceX claims that if reusable rockets are commonplace in the market, payload delivery price will likely decline by orders of magnitude, given that fuel only consumes around $200,000 and the rocket itself amounts to roughly the same price as an airplane to manufacture. SpaceX. "Reusability." https://www.spacex.com/reusability-key-making-human-life-multi-planetary. Caughill, P. "Rocket Lab Has Successfully Launched its Electron Rocket Into Orbit." *Futurism.* Jan. 23, 2018. Sheetz, M. "Morgan Stanley Joins Venture Firms Betting Space Start-up Vector Can Launch A Lot of Small Rockets." *CNBC.* Oct. 19, 2018.

susceptible to increased effects of radiation at high altitudes – such as ephemeral single event upsets (SEUs). SEUs are induced by a flux of cosmic radiation through the on-board circuitry and often result in damage to a single line of computation. For instance, if a neutron collides with a transistor at a sensitive junction, the transistor may release its charge and invert its logical state. The frequency of these insults depend on a variety of physical factors, such as the density of transistors on each chip and the materials utilized for shielding.[129] Nonetheless, COTS incorporation likely decreases the functional lifetime of satellites and contributes to substantial debris generation, a circular consequence of increased rates of deployment and frequent satellite retirement.

In sum, reduction in cost across the supply chain, from launch to satellite construction, allows actors with varying levels of financial resources to deploy satellites to orbit. Where possible, multilateral use of satellites – between combinations of emerging private entities – may be economically advantageous and increase the persistence of services. In particular, satellite operators could use one another as data-links or in-orbit repeaters for

[129] Notably, on October 7, 2008, a Qantas airplane traveling to Singapore allegedly sustained an SEU which caused the plane to quickly and unexpectedly lose altitude. Unrestrained persons were ejected from their seats, leading to the injuries of at least 110 of 303 passengers and 9 of 12 crew members. At cruising altitude, increased radiation caused a logical bit to flip in a plane's inertial reference unit, relaying false information to the plane's control systems and initiating a rapid decrease in altitude. Moreover, at 60,000 feet, the number of neutrons that pass through each square yard of a typical airplane every second is 2,000 times the flux at sea level, and the threat of neutrons to devices in orbit is no less intense. Cooper, N. "The Invisible Neutron Threat." Los Alamos National Laboratory: National Security Science. https://www.lanl.gov/science/NSS/issue1_2012/story4full.shtml. Further, according to a NASA report, the Gravity Probe B (GP-B) spacecraft, launched to study general relativity, suffered an algorithmically uncorrectable multi-bit upset once every 40 days per computer on board. In some cases, if the error was at a critical location, GP-B could only resolve the issue through a total reboot. Compared to COTS hardware, radiation-hardened equipment is specifically designed to mitigate the effects of radiation, and its utilization can prevent upsets like that sustained in flight by Qantas or in space by GP-B. However, radiation-hardened components have a small market and require unique assembly, driving up costs. For instance, a popular radiation hardened processor, the RAD6000, costs at least $200,000, maintains a clock cycle of 25 MHz, and contains roughly 1 million transistors. As a comparison, the Intel Pentium 4, which supports Department of Defense approved encryption, costs $500, maintains a clock cycle of greater than 2 GHz, and contains roughly 55 million transistors. Thus, the non-hardened device is orders of magnitude less costly and delivers much more computing power. In fact, the aforementioned NASA report asserts that radiation hardened hardware lags about a decade behind non-hardened electronics. Mehlitz, P. and Penix, J. "Expecting the Unexpected – Radiation Hardened Software." NASA Ames Research Center publication. https://ti.arc.nasa.gov/m/pub-archive/1075h/1075%20(Mehlitz).pdf.

enhanced line of sight communication. However, to do so requires mutual consideration for how partner constellations network their satellites.

For example, the Iridium and Globalstar constellations provide similar connectivity for telecommunications devices, but operate independently due to design phase decisions which may unnecessarily isolate their constellations. Iridium operates a constellation of 66 functional satellites – along with 6 inactive space-based spares – for global satellite communication.[130] The satellites cross-link to create a mesh network, providing ubiquitous service from geostationary orbit (GEO). Iridium's cross-link capabilities, with the assistance of ground-based gateways distributed across at least 11 different countries, deliver network coverage to remote areas, including polar areas and international waters. The satellites relay packets of information from a Iridium-capable device to a limited number of ground stations. The ground stations then use existing, ground-based means of communication to parse the information and respond accordingly.[131] Globalstar, on the other hand, which offers the same telecommunications services as Iridium, generates a different flow of information.

Globalstar employs a constellation of 48 functional satellites, along with four spares, and 24 ground stations to cover 80% of the Earth's surface.[132] To avail of the service, a user transfers packets of information from a Globalstar-supported device to a Globalstar satellite. The satellite then relays the packets to one of the ground gateways for processing.[133] The absence of cross-linked communication decreases coverage, but also decreases the amount of latency associated with each transmission and subsequently the

[130] Iridium. "Overview Everywhere Under the Sky." Accessed: May 2019. https://www.iridium.com/network/globalnetwork/.

[131] Gupta, O. "Iridium, A Global Communication Network." Slides to Presentation in AA27, Innovation in Aerospace and Space Exploration, Stanford University.

[132] Aerospace Technology. "Globalstar Communication satellite." Accessed Apr. 2019. https://www.aerospace-technology.com/projects/globalstar/; Globalstar. "Our System." Accessed: May 2019. https://www.globalstar.com/en-us/corporate/about/our-technology.

[133] *Ibid.*

likelihood of errors in transmission. Thus, while Iridium enables a data rate of 2.4 kbps and supports wider coverage, Globalstar, managing fewer relays, can exploit terrestrial systems to host a data rate of 9.6 kbps.[134]

However, only U.S. Department of Defense connections appear to be encrypted from end-to-end, based on information provided in a Stanford University report on Iridium's NEXT constellation which only mentions encryption under Defense Department trends.[135] The aforementioned may indicate a difference in security standards between commercial Iridium encryption and DOD requirements. Like GPS, delivering distinct cryptographic keys to all commercial devices would easily grow to be impractical. Commercial communication may be encrypted from the Iridium satellite to the ground-based gateway – utilizing symmetric key predistribution – but threads from commercial devices to commercial gateways may not be encrypted. Distribution of unique keys to every commercial device would be untenable, and asymmetric cryptography would increase the latency of secure communication to GEO substantially. Further, if up- and down-link communication is encrypted, the cryptographic key(s) are likely to be constant for all communication, meaning if an adversary discovers the key, he can intercept and decrypt all consumer exchanges. Since the Defense Department likely operates fewer devices than the sum of commercial consumers, the DOD may, with difficulty, support key distribution.[136]

In the event that a satellite sustains damage in orbit, leading to a loss of function, Iridium and Globalstar plan to activate one of their respective spare satellites already orbiting the globe. The spare will likely be chosen based on its location, facilitating

[134] Bluecosmo. "Satellite Network Comparison Table." Accessed: May 2019. https://www.bluecosmo.com/compare-satellite-networks.

[135] Gupta, O. "Iridium, A Global Communication Network." Slides to Presentation in AA27, Innovation in Aerospace and Space Exploration, Stanford University.

[136] de Selding, P. "Iridium to Update Hawaii Gateway for Pentagon." *Space News.* Oct. 31, 2012.

reassembly of global coverage. However, relocating a satellite to reestablish service possess an associated latency and may require additional support from ground-based actors.

For instance, Panamsat's Galaxy 4 had a system error in 1998 that caused roughly 45 million pagers to lose service.[137] Panamsat required six days to relocate another satellite, the Galaxy 6, from its original orbit in order to replace the Galaxy 4. In addition, Panamsat instructed 3,500 workers to redirect 25,000 satellite dishes in order to connect to the Galaxy 6 – which required some customer traffic to be rerouted through a different satellite, the Galaxy 3R.[138] Here, limited redundancy was helpful. If Panamsat did not have other satellites with the freedom to assume extra responsibility, the Galaxy 4 incident could have been much worse. Even so, the manpower and time to resolve the issue could have been reduced if Panamsat held additional redundancy at its disposal.

Notably, there may be cases where the aforementioned redundancy does not necessarily have to originate from native Panamsat satellites. The same holds for Globalstar and Iridium – so long as they are communicatively interoperable. Native, internal redundancy not only increases procurement costs, but also enhances concerns pursuant to Articles VI, VII, IX, and XI of the Outer Space Treaty. As additional constellations are deployed, a stronger hardware footprint in orbit emerges, deepening as satellites are decommissioned and replacements are deployed; thus, the case for cross-constellation cooperation is only likely to increase as time and technology advance.

[137] Madrigal, A. "The Great Pager Blackout of 1998." *The Atlantic.* Mar. 25, 2011.

[138] Zuckerman, L. "Satellite Failure is Rare, and Therefore Unsettling." *New York Times.* May 21, 1998.

Conclusion

Differences in on-board equipment, required resources, and informations security may preclude robust interoperability between some systems, such as those used for national security and those which have very specialized mission sets. However, actors which are not encumbered by the aforementioned may cooperate to increase the persistence of their services and limit the number of objects deposited to orbit. Currently, there is limited guidance on how this is to be practically executed; however, examination of how operators in other sectors collaborate to distribute a common service across international borders may provide valuable insight.

The behavior of entities deploying and utilizing undersea cables may assist policy makers in developing an enforceable, market optimal means for satellite operators to adhere to best practices for activities in outer space. Privately owned networks of undersea or submarine fiber-optic cables transmit terabytes of data per second, ensuring the persistence of cross-continent connectivity. Moreover, similar to the laws governing outer space, the guidelines surrounding submarine cables lack enforceability, relying on states to pass legislation mirroring drafted resolutions. Even so, cable operators appear to adhere to such guidelines as a product of mutual interest, cooperating with one another to ensure the resiliency of their collective coverage.

Ultimately, the features which allow for such cooperation distill to the standardization of equipment, which facilitates redundancy and the reproducibility of damaged components. The following case study details the laws and guidelines which govern the behavior of undersea cables, the risks to undersea cables, and the features which can be extracted to serve actors in outer space.

3.2.1 Case Study: Undersea Cables

In 1858, U.S. President James Buchanan and Queen Victoria routed messages through an undersea cable to exchange the fastest trans-Atlantic telegram of their time.[139] Contemporary processing techniques required roughly 17 hours to recover the message, but today, undersea cables transmit 97% of intercontinental digital traffic, including $10 trillion of daily financial transactions.[140] Nevertheless, submarine cables must operate in a global domain governed by a web of international law, plagued by the same issues facing all UN and other arrangements. Notably, submarine cables are mostly operated by commercial actors, generating difficulties in diplomatic representation and choice of law which also arise in the laws of outer space. This section first landscapes the international laws which govern undersea cable operation, comparing relevant provisions to those which relate to outer space. Further, this section analyzes areas of standardization, redundancy, and interoperability in the sector which have not necessarily resulted from international *legal* agreements, but may similarly translate to cross-constellation satellite networking, delivering an enhanced, collective ability to deliver persistent data throughput.

The first effort to facilitate international cooperation and discourse surrounding undersea cable maintenance, which 27 states attended and signed, was the 1884 Convention for the Protection of Submarine Telegraph Cables ("1884 Convention").[141] The provi-

[139] History.com Editors. "First Transatlantic Telegraph Cable Completed." *A&E Television Networks.* Last updated: Feb 25, 2019. https://www.history.com/this-day-in-history/first-transatlantic-telegraph-cable-complete

[140] U.S. Department of Homeland Security and Office of the Director of National Intelligence. "Threats to Undersea Cable Communications." Sept. 28, 2017. Meyer, R. and Starosielski, N. "Managing Risks for the World's Undersea Cable Network." University of Pennsylvania, Knowledge at Wharton podcast. Nov. 2, 2015. Lavallée, B. "The Story Behind the First Reliable Trans-Atlantic Submarine Cable Laid 150 Years Ago." Ciena Publication. Jul. 14, 2016. Sunak, R. "Undersea Cables: Indispensable, Insecure." *Policy Exchange.* Dec. 1, 2017.

[141] Protection of Submarine Cables, Library of Congress, 24 Stat. 989, Treaty Series 380, Mar. 14, 1884.

sions therein outline how states and commercial actors are to interact with undersea cables. For instance, Article II of the 1884 Convention states that "The breaking or injury of a submarine cable, done willfully or through culpable negligence, and resulting in the total or partial interruption or embarrassment of telegraphic communication, shall be a punishable offense."[142] The text additionally creates a one nautical mile buffer zone between any ship and an undersea cable undergoing repairs via another ship or a series of buoys indicating a damaged undersea cable. Notably, in the event that a ship damages a cable, the 1884 Convention apportions culpability to the party which exacted the injury.[143] Unlike COPUOS in 1967, the 1884 Convention is assigns culpability to the aggressive or negligent party, not the state government ostensibly supervising the activity. This is likely a derivative of the difference in historical ownership of undersea cables and spacecraft. Even for decades after delivering objects to space was feasible, spacecraft were exclusively owned, operated, or sponsored by state governments. However, undersea cables are most often owned by private entities or groups of private entities. Even the undersea cable used by President Buchanan and Queen Victoria was privately owned by the Atlantic Telegraph Company.[144]

Other international efforts, such as the 1982 United Nations Convention on the Law of the Sea (UNCLOS), address undersea cables in a more modern light.[145] Article 112 of UNCLOS provides every state the right to lay undersea cables, and Articles 113-114 assert that governments which ratify the text agree to create laws making willful or negligent damage to such cables a punishable offense.[146] However, in the event of an international dispute, the aggrieved party may have to convince its host nation to diplomatically settle

[142] *Id.* at art. 2.

[143] *Id.* at art. 4.

[144] Sunak, R. "Undersea Cables: Indispensable, Insecure." *Policy Exchange.* Dec. 1, 2017.

[145] United Nations Convention on the Law of the Sea, Dec. 10, 1982, 1833 U.N.T.S. 3.

[146] *Id.* at art. 112-114.

the dispute. In other words, as with the choice of law challenge that plagues the Outer Space Treaty, private entities are able to choose their host nation and the attached *legally enforceable* framework.

Outside of state sponsored efforts to secure and manage undersea cable operations, 97% of all undersea cables are represented by their operators within the International Cable Protection Committee (ICPC).[147] The ICPC Vision Statement is "[t]o be the international submarine cable authority providing leadership and guidance on issues related to submarine cable security and reliability."[148] Similar to the IADC and space agencies, stakeholders join to provide interest-driven input on responsible deployment and repair of the cables. Even entities which do not deploy cables are a party to the ICPC. For instance, JP Morgan Chase and Goldman Sachs are active members, likely to advocate for the high degree of security, maintenance, and interoperability which sustains their respective transactions.[149]

Nonetheless, the most effective collaborative efforts to increase the persistence of service likely results from equipment and protocol standardization. While many service providers invest in the construction of undersea cables, there are four primary companies who supply the lines: Nokia (Alcatel-Lucent), NEC, TE-Subcom, and Huawei Marine.[150] However, optical equipment to interpret the signals at cable landing points is manufactured by several companies from different states – including the U.S., France, China, and Japan.[151] The lack of diversity in physical structure of the lines leads to an implicit standardization in the process to deploy, manage, and repair the lines.

[147] International Cable Protection Committee. Accessed: May 2019. https://www.iscpc.org/.

[148] For statement, see: https://www.iscpc.org/about-the-icpc/vision-statement/. Accessed: May 2019

[149] For members, see: https://www.iscpc.org/about-the-icpc/member-list/. Accessed: May 2019.

[150] U.S. Department of Homeland Security and Office of the Director of National Intelligence. "Threats to Undersea Cable Communications." Sept. 28, 2017.

[151] *Id.*

According to TeleGeography, there are roughly 378 operational undersea cables, but this number changes frequently as lines are retired and others are commissioned.[152] In total, there are around 1 million kilometers of cable lining various depths of the ocean.[153] Although, entities reuse existing terrestrial infrastructures where possible. For instance, the Virginia Beach Cable Landing Station currently serves the BRUSA, Durant, MAREA, and South Atlantic Express (SAEx1) submarine cables.[154] The station itself is owned by Telxius, but the cables are owned and operated by combinations of Telxius, Google, Microsoft, Facebook, and SAEx International.[155] Nonetheless, reuse of common landing points creates regional chokepoints in the system, heightening the importance of security at each landing station and around the dense clusters of cables which connect to them – just as monolithic satellites create chokepoints in their associated systems.[156]

In addition to the interoperability observed at landing stations, cable operators sometimes choose to join consortiums to reroute information from their cables to other networks in the event of a breakage – a feature which is discounted without technical interoperability. For instance, the South-East Asia Japan Cable (SJC) System consortium comprises 11 cable owners which connect seven landing stations in six countries, and the

[152] TeleGeography. Submarine Cable Frequently Asked Questions.
https://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions
Accessed: Apr. 2019. This estimate is as of early 2019.

[153] *Ibid.*

[154] See: https://www.submarinenetworks.com/en/stations/north-america/usa-east;
https://www.submarinecablemap.com/#/landing-point/virginia-beach-va-united-states;
Miller, R. "Another Data Center Planned for Virginia Beach Cable Landing." *Data Center Frontier.* Apr. 28, 2019.

[155] *Ibid.* all.

[156] Natural and malicious events targeted at such chokepoints can result in a loss of coverage or throttle access to timely information. For instance, an earthquake in Taiwan in 2006, touching 7.0 on the Richter scale, severed 8 cables in 18 distinct locations connecting Taiwan and the rest of the world. Qiu, W. "Submarine Cables Cut after Taiwan Earthquake in Dec 2006." *Submarine Cable Networks.* Mar. 19, 2011. The event resulted in a loss of 98% of the communication from Malaysia, Thailand, Singapore, and Hong Kong until the lines were repaired 49 days later – the latency was likely due to the number of fractures and the relatively deep locations of some of the damaged cables. *Ibid.*; Meyer, R. and Starosielski, N. "Managing Risks for the World's Undersea Cable Network." University of Pennsylvania, Knowledge at Wharton podcast. Nov. 2, 2015; Shan-Hun, C. "Communications chaos in Asia after quake hits Taiwan-Asia-Pacific-International Herald Tribune." *New York Times.* Dec. 27, 2006.

Southeast Asia–Middle East–Western Europe (SEA-ME-WE 5) consortium consists of 15 cable operators which connect 17 countries.[157] The SJC and SEA-ME-WE 5, with common equipment from NEC, TE-Subcom, and Alcatel-Lucent, intend to mitigate damage to any one of their lines through built in network redundancy, exploiting the compatibility between the physical and network features common throughout their respective consortiums. So if one region of the system breaks, traffic is rerouted through different cables to ultimately reach the destinations that would be primarily served by the broken cable.[158]

To ensure the utility of redundancy, cable operators intentionally reserve bandwidth on their lines. For instance, MainOne delivers data at 1.92 Tbps, but is capable of nearly 5 Tbps.[159] So if needed, MainOne may be able to assume the transmission responsibility of a nearly identical cable. In the end, the aforementioned corsortiums and others create network redundancy ensure that a limited number of disconnections are unnoticeable to end users.[160] Further, to support the swift repair of cables after a fracture, operators engage in collectively funded maintenance agreements.[161]

Arrangements, such as the Atlantic Cable Maintenance Agreement (ACMA) and the Mediterranean Cable Maintenance Agreement (MCMA), arise from a wide interest in the

[157] South-East Asia Japan Cable (SJC) System Overview. *Submarine Cable Networks.* Aug. 12, 2011. https://www.submarinenetworks.com/systems/intra-asia/sjc/sjc-cable-system; Winston, Q. "SEA-ME-WE 5 Consortium Concludes Construction Agreement." *Submarine Cable Networks.* Mar. 10, 2014.

[158] Coffey, V. "Sea Change: The Challenges Facing Submarine Optical Communications." *The Optical Society: Optics and Photonics.* Mar. 2014.

[159] For MainOne information, see: https://www.africafc.org/What-We-Do/Projects/Main-One.aspx. Accessed: Apr. 2019.

[160] Note, service may slow as a limited number of cables become congested or traffic must matriculate through a chain of relatively more distant cables. Further, traffic may close completely if the system lacks the ability to reroute communication.

[161] A report prepared for a U.S. Department of Homeland Security official claims a cable fractures occurs somewhere in the world once every three days. Sechrist, M. "Cyberspace in Deep Water: Protecting Undersea Communication Cables By Creating an International Public-Private Partnership." Report Prepared for Rand Beers, Under Secretary for National Programs and Protection Directorate, Department of Homeland Security. Mar. 23, 2010.

rapid repair of cable lines with the most regionally available, capable workforce.[162] For instance, the ACMA operates a fleet of three vessels, stationed in the United Kingdom, France, and the Netherlands Antilles, and serves 59 cable operators that have accepted an ACMA contract.[163] As an example, when the MainOne undersea cable sustained damage that needed repair in June 2017, and ACMA officials repaired, tested, and placed the MainOne back in operation roughly two weeks after the break.[164] Notably, repair is facilitated through the standard use of equipment among cables – limiting additional logistical, procurement, and storage requirements – and the trust placed in the ACMA by the cable operators.

Common trust is a theme which permeates throughout many areas in the operation of undersea cables. Trust in the ACMA reduces to similar security requirements among cable operators and further facilitates interoperability. Implicitly, the 59 ACMA members must trust the cable repair officials. In addition, any cables connected to the same landing points or within the same consortium inherently assume similar network risks. Without similar standards, security recalibration would obviate the ability of consortiums to reroute data and undercut the ACMA's ability to quickly repair lines. Namely, entities which transmit data through undersea buses, not the cable providers themselves, are responsible for their own information security. Thus, cable operators are provided flexibility with security, enhancing interoperability and supporting a dedicated focus on

[162] U.S. Department of Homeland Security and Office of the Director of National Intelligence. "Threats to Undersea Cable Communications." Sept. 28, 2017.

[163] For ACMA information: https://www.acma2017.com/about/members/. Accessed: Apr. 2019.

[164] An underwater landslide caused a break in the MainOne cable around 3,000 kilometers south of Portugal, 3,400 meters under the surface. MainOne, based in Nigeria, alerted the ACMA, and a French cable repair ship was enlisted to restore the connection. The French vessel stopped in the United Kingdom to obtain repair supplies, including backup cables, a repeater, and materials to join disparate cables. The vessel arrived at the break 8 days after departing and took 6 days to complete the repair. Miller, J. "Repairing a Damaged Submarine Cable: How MainOne Was Put Back in Service." Telegeography Blog. Aug. 8, 2017.

maintaining the availability of the cables.[165]

Satellite repair is inherently more difficult than undersea cable repair, due to access to the damaged asset. Therefore, agreements like ACMA may not be practical. However, consortiums comprised of entities whose satellites communicate through similar mechanisms – similar up-, down-, and cross-link frequencies, utilization of the same ground-based stations, equivalent signal modulation techniques, mutually agreed upon channel access methods, and other network level features – may provide enhanced service resiliency. In such an arrangement, satellites within a constellation may assume traffic from a distinct constellation which has sustained damage to one of its satellites. Rerouting could continue until the operator of the latter deploys a satellite to replace the damaged asset. Such arrangements would have to be executed on the ground, during the design phase of satellites in order to ensure that mechanisms for communication are compatible. Such an arrangement depends primarily on the interoperability between distinct systems, as well as the amount of time an entity requires in order to replace the damaged satellite.

3.2.2 Satellite-to-Satellite Compatibility

As satellite constellations become increasingly commercialized, agreements analogous to those between undersea cable operators may emerge if there exists sufficient standardization in equipment and network protocols to deliver constellations the opportunity for interoperability. First, this section describes two areas of standardization which can facilitate interoperability at the scale observed with submarine cables: compatibility at the

[165] Concerning privacy and traffic analysis, there is limited control, or even knowledge, related to which undersea cables transmit particular commercial information. Therefore, there is limited expectation that the existence of communication will remain private.

data-link layer across constellations; and interoperability with common terrestrial gateways. Then this section suggests operational agreements which may be possible, provided the aforementioned layers of standardization. Notably, this section does not describe *how* entities are to engage in such agreements or *how* entities will achieve meaningful security over cross-constellation communication. Chapter 4 provides a tool for the latter and Chapter 5 describes how that tool, or one similar, may be utilized to address former – and in the process conform to the previously discussed provisions in the Outer Space Treaty.

A chain of satellites which broadcast within the same frequency bands may simulate the physical data transport mechanism presented by undersea cables. Further, intermediate satellites between communicating nodes may amplify data in transit if mechanisms for modulation and data transmission over a network are standardized, thereby decreasing the likelihood of data loss over long distances. However, satellites do not enjoy the inherent authentication provided between amplifiers within physical confines of undersea cables. As a result, satellites relaying information between one another, even if that data is not semantically interpreted, likely require a method for authentication and situational coordination to ensure the correct packets are relayed and the order of the packets can be maintained.

Notably, complete interoperability at the level where satellites can semantically interpret information from satellites of disparate constellations is likely impractical. If intermediate satellites parse information, there will be an even larger latency increase and security will have to be standardized among all satellites participating in a single stream of information. However, an infrastructure of connected constellations might not preclude this feature, as some use cases, such as systems for telecommunications, may benefit from this layer of interoperability.

Undersea cable operators enjoy robust cooperation because they are primarily concerned with availability and physical security of the lines, ignoring confidentiality of the communication contained within the cables. Satellite operators intending to achieve complete interoperability would not enjoy such freedom. In the end, satellite-to-satellite compatibility does not necessarily have to be comprehensive. So long as constellations are communicatively interoperable, the degree to which they exchange resources may remain a decision for satellite operators.

Common terrestrial gateways provide advantages in deployment, data processing, and information security. For instance, Iridium operates at least 12 gateways around the world to deliver global coverage, which may feed and receive data to agreed upon constellations. Even if there is not availability within Iridium's 1618.725-1626.5 MHz bandwidth for up- and down-links, the existing infrastructure which surrounds the gateways, later transporting information to ground-based systems, may be utilized by distinct satellite operators.[166] Nonetheless, as with cross-link communications, satellites must have some method for authenticating themselves to the target destination. This may entail human representatives exchanging information between one another on the ground, later transmitting the material to their respective satellites. However, this approach becomes untenable as the number of constellations grow. In practice, a third-party, which all parties in a particular exchange trust, could mutually authenticate up- and down-link transmissions to ensure that satellites and gateways are permitted to connect to one another.

After technical compatibility is instituted, participation in organizations which pro-

[166] Gupta, O. "Iridium, A Global Communication Network." Slides to Presentation in AA27, Innovation in Aerospace and Space Exploration, Stanford University.

mote the persistence of the group's services can emerge. Maintenance agreements, like stipulations within the ACMA, are likely impractical in outer space. *Repair* of damaged cables cannot feasibly translate to *repairing* dysfunctional satellites. However, with decreasing costs to manufacture and launch, the feasibility of *replacing* a damaged asset in a timely manner may become more of a reality – leading to the practicality of constellation-to-constellation redundancy, or external redundancy.

Some constellations incorporate additional satellites for internal redundancy, but deploying redundant satellites increases operating costs and exacerbates concerns associated with the articles of the Outer Space Treaty highlighted above – Articles VI, VII, IX, and XI. As previously discussed, Iridium and Globalstar retain in-orbit spare satellites to prevent service disruption, but each bus requires continued supervision according to Article VI, increases the likelihood of accidents and the subsequent liability attached by Article VII, and may eventually create debris that threatens other assets or the fair use of the domain, despite limited use.

Nonetheless, redundancy has obvious benefits. As previously mentioned, Panamsat, which sustained minimal redundancy, could have mitigated the effects of losing the Galaxy 4 through simply having more assets deployed.[167] However, such redundancy does not necessarily have to reside within an actor's constellation.

For instance, the Sierra Nevada Corporation controls a constellation of eight satellites to enhance early weather forecasting, allowing experts to, for instance, timely and accurately predict hurricane behavior.[168] In this case, due to the nature of the service, the disablement of a limited number satellites would likely not pose a large risk to the service overall – assuming there is not a pending natural disaster that requires constant

[167] *Supra* notes 138-139.

[168] Sierra Nevada publication. "Revolutionary New Hurricane Satellite System Supported by Sierra Nevada Corporation." Dec. 15, 2016. https://www.sncorp.com/press-releases/snc-cygnss/.

satellite monitoring. Thus, Sierra Nevada could enter into an agreement with an entity, like Panamsat, to form a system with out-of-constellation redundancy – so long as the satellites of each constellation can minimally communicate with one another. This type of agreement asserts that Sierra Nevada may provide Panamsat with satellites under certain pre-specified conditions. Under a few significant technological and security assumptions, this form of redundancy can be an effective means to mitigate the effect of damaged satellites.

Notably, government endeavors may be in a position where external redundancy could be an effective boost to ongoing pursuits of internal redundancy, given that commercial space development is racing ahead of the public sector's pursuits and single, monolithic satellites may present vulnerabilities in physical security. A barrier in information security may remain, but contemporary command of autonomous systems, Internet of Things devices, and sophisticated electronics for warfighting demand bandwidth which existing satellites may already offer, leaving an opportunity to exploit forward-deployed, low-cost systems.

Today, there are many companies operating space systems who may be amenable to agreements which forge external redundancy. Notably, INTELSAT, INMARSAT, Iridium, SES, Globalstar, Orbcomm, and others provide similar telecommunications and tracking services, each of which is slightly unique, but future iterations could observe measures for interoperability. Regardless, all of the aforementioned intend to provide customers with a reliable service that customers can count on in emergency or tactical situations.

In the end, if combinations of commercial and government satellite operators wish to engage one another like the undersea cable community, equipment and approaches to transmit information across constellations, or with other receiving nodes, must be interoperable. To do so, satellites must share similar technical features, such as similarly sized antennae, modulation techniques, and other network techniques which entail significant design phase collaboration. Assuming satellites in distinct constellations can either communicate with one another or simply act as passive relays, space-based systems will need a mechanism to mutually authenticate – and possibly exchange confidential information between – one another. As a basis for the aforementioned, one needs a key management protocol to coordinate protected communication between distinct satellite systems and between space- and ground-based nodes.

4 Kerberized Identity-Based Encryption (KIBE)

Kerberized Identity-Based Encryption (KIBE) is a possible key management solution for communication within an infrastructureless network, such as that forged by a constellation of satellites. Nodes may dynamically enter and exit the network, requiring communication to be spectrally efficient and reliable. In order to address physical challenges in bandwidth, propagation delay, intermittent connectivity, and hardware resources, as well as facilitate protected cross-constellation communication, KIBE addresses the following:

1. **One cross-link transmission is sufficient to both negotiate a shared key and encrypt a message.** In some asymmetric key exchanges, parties exchange multiple messages in order to negotiate a secret, a suboptimal feature given an infrastructureless network topology. To reduce the number of messages exchanged, systems may standardize the security association and store the public keys for all parties in the constellation. However, this forecloses the opportunity to flexibly respond in the event that a security assumption is no longer valid. Additionally, rotating key pairs for forward secrecy would require substantial redistribution of public key material to all satellites, a process which becomes untenable as the constellation grows.

2. **Cryptographic material will not require predistribution for cross-link communication.** The simplest solution to secure communication within a constellation is to provide each satellite with an identical symmetric key – at the expense of creating a single point of failure. A slightly improved approach may be

to provide each satellite pair with a unique symmetric key. Although, when a new satellite joins the constellation every satellite must receive a new symmetric key in order to communicate with the recently introduced node. The same round of key distribution would have to occur for key revocation in the event that a satellite is compromised. Additionally, every satellite in the system would have to trust the same party to predistribute keys, delivering this party an escrow into any cross-link communication. KIBE requires that each satellite possess a single, unique symmetric key shared with a ground-based entity; however, satellites in the system are not required to store overlapping cryptographic material, and requirement 4 below addresses the escrow.

3. **Any authentication protocol to a ground station over the air must be limited in the number of exchanges, keys for authentication will not be predistributed, and artifacts for certification must expire after a specified time. In addition, symmetric cryptography should be utilized where possible in order to reduce latency and ciphertext expansion.** Third-party certification must be limited to avoid lengthening the latency between the decision to send a message and the destination satellite's receipt of the message. Predistribution of keys for authentication becomes impractical as the constellation grows for the same impracticalities associated with predistribution for confidentiality described above.

4. **An authority for authentication must not have a key escrow into the communication between parties which it certifies, unless the ability is desired.** Despite trusting an entity for identity certification in some cases, access to the communication may not be desired. Symmetric protocols like Kerberos

inherently create a key escrow. Thus, a limited amount of asymmetry must be employed to remove the escrow and prevent the need for key predistribution.

Given the above, this paper intends to present a key management protocol which utilizes identity-based encryption (IBE) and draws parallels to the Kerberos protocol for authentication. KIBE allows entities which posses a certificate and token to exchange a symmetric key, encrypt a message, and authenticate the message in a single transmission. Further, forward secrecy with respect to each key pair can be maintained without distributing new keys to every other node, and different constellations are permitted to utilize distinct cryptographic security assumptions.

First, this paper discusses identity-based encryption and the bilinear pairing operations which support this study's implementation. The next section describes the Kerberos protocol for symmetric authentication, and the following portion illustrates existing key management protocols for identity-based encryption and highlights their differences relative to this study's protocol. Afterward, this study assesses KIBE and its implementation.

4.1 Identity-Based Encryption

Identity-based encryption (IBE), first suggested by Shamir in 1984, is a variant of public-key cryptography with arbitrary public keys and a system master secret, typically employed, in whole or in part, to generate each private key.[169] For instance, a public key can be a social security number, email address, or other assigned identifier. Notably, private keys may be refreshed while the public key remains constant through altering the system secret. Alternatively, using the same system secret, public keys can be adjusted in

[169] Shamir, A. "Identity-based cryptosystems and signature schemes", *Advances in Cryptology – Crypto '84*, Lecture Notes in Computer Science, Vol. 196, Springer-Verlag, pp. 47–53, 1984.

a predictable manner, requiring a new private key but discounting the need for partners to query the party for a new public key. Nonetheless, either of the aforementioned enables forward secrecy.

The NIST notes that "IBE simplifies key management procedures of certificate-based public-key infrastructures," indicating that IBE may be used when a context presents key management challenges.[170] The security assumption supporting the protocol ensures that only recipients with the desired identity will be able to decrypt the true message. In other words, identities are inherently certified when they are provided to every node, given a set of system certified public parameters. Therefore, so long as a sender certifies the public parameters or is within the purview of the PKG, the initiator is able authenticate the receiver by nature of encryption.

IBE systems comprise four algorithms: (1) `Setup`; (2) `Extract`; (3) `Encrypt`; and (4) `Decrypt`. Both `Setup` and `Extract` are performed by a trusted entity, known as the Private Key Generator (PKG). The algorithms are generally as follows:

1. `Setup`(λ) : Input the security parameter λ and output public parameters $\mathcal{P}$ and master secret s.

2. `Extract`$(\mathcal{P}, s, ID)$: Input the public parameters, master secret, and an identifier ID for a particular node in the system. This identifier is the selected public key for the stated node. Output the corresponding private key pk_{ID}.

3. `Encrypt`$(ID, \mathcal{P}, m)$: Input the destination node's identifier, public parameters, and message m. Output ciphertext c.

[170] Moody, D. et al. "Report on Pairing-Based Cryptography." *Journal of Research of the National Institute of Standards and Technology.* Feb. 3, 2015.

4. $\texttt{Decrypt}(c, \mathcal{P}, pk_{ID})$: Input the ciphertext, public parameters, and private key. Output the decrypted message m.

For example, email addresses may embody the system public keys. In this case, if Alice wishes to email Bob, Alice can encrypt a message using Bob's email address. To decrypt the message, Bob authenticates himself to the PKG, which subsequently issues Bob his private key.[171] Note, Alice can send a protected message to Bob before Bob has received his private key; however, it remains to be seen how Alice authenticates herself to Bob. In addition, the PKG has an inherent escrow into all communication that Bob receives.

To allow for the expiration of public keys, one may append timestamp to the public key. For instance, Bob's public key may become `Bob@example.com||expiration`, which would require extraction of a new private key.[172] IBE can also manage access to distinct functions offered by the receiver. For instance, Bob's public key may become:

`Bob@example.com||expiration||func=telecommunication`,

preventing Bob from decrypting messages encrypted using a public key comprising a different expiration or function.

Moreover, satellites in a constellation can retain a plurality of transient identities to accomplish an objective. For instance, assume an actor intends two satellites to work in concert for a limited time in order to accomplish `objective A`. Each satellite can simply assume the public key `objective A`, while the PKG issues each satellite the corresponding private key for `objective A`. After the objective has been accomplished, the PKG may,

[171] Boneh, D., Franklin, M. "Identity-Based Encryption from the Weil Pairing." *SIAM Journal of Computing*, vol. 32, No. 3, pp. 586–615. 2003.

[172] *Id.*

for instance, issue each satellite distinct public keys for distinct objectives, extracting the appropriate private keys for each.

Security for public-key methods is often met through protecting against chosen plaintext attacks. If chosen plaintexts are indistinguishable after encryption, the scheme achieves CPA-security or is labeled IND-CPA secure. Note, a scheme that meets a meaningful level of CPA-security is implicitly semantically secure. To demonstrate CPA-security, an adversary and a challenger play the following game: 1) the adversary sends a challenger m_0 and m_1, such that $m_0 \neq m_1$ and the messages are of equal length; 2) the adversary queries the challenger on a polynomial number, with respect to the security parameter, of plaintexts, and the challenger provides the corresponding ciphertexts; 3) the challenger randomly chooses $b \leftarrow \{0, 1\}$, encrypts $c = m_b$ with some public key, and sends c to the adversary; and 4) the adversary attempts to identify which message was encrypted and outputs b'. If $b = b'$, then the adversary wins. Thus, the scheme is IND-CPA secure if the adversary has negligible advantage.

A stronger definition arises if the adversary can adaptively query the challenger after receiving the encrypted challenge. For instance, after receiving c, the adversary can further query the challenger to encrypt any messages other than m_0 and m_1. After a polynomially many number of queries, the adversary then outputs its guess b'. Security against adaptively chosen plaintexts is referred to as CPA2-security. Nevertheless, CPA- and CPA2-security may be thought of as semantic security. Within the game, the adversary can design m_0 and m_1 to assume distinct semantic meanings, and if the adversary is able extract information from c, beyond negligible advantage would be provided.

Security for IBE protocols is defined through a slightly different game in order to achieve indistinguishability for chosen identities and plaintexts, known as IND-ID-CPA-security. Here, one allows the adversary to query the challenger regarding not only different messages, but also different public keys – or identities. The IND-ID-CPA game between a polynomial time adversary and the challenger is the following:[173]

1. The challenger embodies the PKG and executes the `Setup`. The challenger issues the adversary the necessary public parameters.

2. The adversary asks the challenger to extract private keys for a polynomial number of IDs. After each query, the challenger sends the adversary the extracted private key, pk_{ID}.

3. Once the adversary is content, the adversary sends the challenger distinct, equal length messages m_0 and m_1 and some ID^* that was not queried in the previous phase. The challenger randomly chooses $b \leftarrow \{0, 1\}$ and encrypts m_b using the given ID^* and public parameters from `Setup`. The challenger provides the ciphertext c to the adversary.

4. The adversary is able to ask for more private key extractions for IDs that are not equal to ID^*.

5. The adversary outputs b'

As before, the adversary wins if $b' = b$. The protocol is IND-ID-CPA secure if the adversary is provided negligible advantage over random guessing.

[173] *Id.*

Definition 1. *A scheme is adaptively secure against chosen plaintext attacks, or IND-ID-CPA secure, if for any polynomial time adversary A, the following holds:*

$$Pr[A(ID^*, c) = b' | b' = b] \leq \frac{1}{2} + \epsilon$$

where ϵ is negligible.

There exists still a stronger notion of security – chosen ciphertext security (CCA-security). A replay attack, or variant thereof, can be thought of as chosen ciphertext attack. For instance, if an adversary is able to determine that a subset of ciphertexts $H \subseteq C$ elicits a response from the challenger, the challenger can be exploited. An adversary may selectively choose to send $c \in H$ or $c' \in C \setminus H$ to gain advantage. In total, a CPA-secure encryption scheme with an unforgeable signature scheme achieves CCA-security.

Ultimately, if an adversary can view decryptions of chosen ciphertexts without gaining noticeable advantage, the scheme achieves CCA-security or indistinguishability under chosen cipertexts (IND-CCA security). A traditional CCA-security game may proceed as follows: 1) the adversary sends a challenger m_0 and m_1 such that $m_0 \neq m_1$ and the messages are of equal length; 2) the adversary queries the challenger on a polynomial, with respect to the security parameter, number of ciphertexts, and the challenger provides the corresponding plaintexts; 3) the challenger randomly chooses $b \leftarrow \{0, 1\}$, encrypts $c = m_b$ with some public key, and sends c to the adversary; and 4) the adversary attempts to identify which message was encrypted, outputting guess b'. If $b = b'$, then the adversary wins. The scheme is IND-CCA secure if the adversary has negligible advantage. CCA2-security involves the same modificatin from CPA- to CPA2-security: adaptive queries after the randomly chosen challenge message was encrypted and sent to the adversary.

For IBE, we modify the game so that the adversary can adaptively query different

IDs and extract their corresponding private keys – as performed in the IND-ID-CPA game. The IND-ID-CCA game is the following:[174]

1. The challenger embodies the PKG and executes `Setup`. The challenger issues the adversary the necessary public parameters.

2. The adversary issues a polynomial number of queries to challenger oracles which perform either of the following:

   (a) $\mathcal{O}^{ID}$: Extracts the private key pk_{ID} for queried ID

   (b) $\mathcal{O}^{ID,c}$: Decrypts some ciphertext c with the private key corresponding to queried ID

3. Once the adversary is content, the adversary sends the challenger distinct, equal length messages m_0 and m_1 and some ID^* that was not queried in the previous phase. The challenger randomly chooses $b \leftarrow \{0,1\}$ and encrypts m_b using the given ID^* and public parameters from `Setup`. The challenger provides the ciphertext c to the adversary.

4. The adversary can execute the same queries as in step 2.

5. The adversary outputs b'

The adversary wins if $b' = b$. The protocol is IND-ID-CCA secure if the adversary is provided negligible advantage over random guessing.

[174] *Id.*

Definition 2. *A scheme is adaptively secure against chosen ciphertext attacks, or IND-ID-CPA secure, if for any polynomial time adversary A, A exhibits the following:*

$$Pr[A(ID^*, c) = b'|b' = b] \leq \frac{1}{2} + \epsilon$$

where ϵ is negligible.

Boneh and Franklin give IND-ID-CPA and IND-ID-CCA versions of their IBE protocol, both of which require bilinear pairings over elliptic curve elements.

4.1.1 Bilinear Pairing

A bilinear pairing, or bilinear mapping, is an operation performed on a pair of elements of certain groups which transforms the pair into an element of a distinct group. In other words, for groups G_1, G_2, and G_t, e is a bilinear mapping from G_1 and G_2 to G_t:

$$e : G_1 \times G_2 \rightarrow G_t$$

Note, practitioners focus on permissible mappings where e exists and is efficiently computable. Further, for cryptographic application it is often the case that $G_1 = G_2$. In order for the mapping to be permissible for the Boneh-Franklin protocol, where $G_1 \times G_1 \rightarrow G_t$, the following must hold:[175]

1. For $P \in G_1$ and $Q \in G_2$ where G_1 and G_2 have prime order q, with $a, b \in \mathbb{Z}_q^*$, the following holds:

$$e(aP, bQ) = e(abP, Q) = e(P, abQ) = e(P, Q)^{ab}$$

[175] *Id.*

2. The mapping is non-degenerate. In other words, the pairing does not map all results to the identity in G_t. Further, if P is a generator of G_1, then $e(P, P)$ is a generator of G_t.

3. The mapping must be efficiently computable.

If the above are satisfied, one has found an admissible bilinear mapping for the Boneh-Franklin IBE scheme. Boneh and Franklin utilize the Weil pairing for elliptic curve elements, and the product with this paper builds the protocol using the Tate pairing. There is little difference between the two, but the Tate pairing is known to be slightly faster.[176] Nevertheless, pairing algorithms for elliptic curves tend to be relatively slow, and improvements therein remain an active area of research.

Beyond choosing admissible elliptic curves, one must examine the security espoused by each curve. Both G_1 and G_t must meet standards for a secure scheme. As previously noted, the MOV reduction shows that computing the logarithm of elliptic curve point addition in G_1 is no harder than computing the discrete logarithm in G_t for certain elliptic curves. In other words, if one has an efficient algorithm to compute the discrete logarithm in G_t, one can use the algorithm to compute the logarithm of elliptic curve elements in G_1.[177]

To illustrate the above, assume that $P, Q \in G_1$ which has prime order q. Further, let $Q = aP$ where $a \in \mathbb{Z}_q^*$. If $g = e(P, P)$ and $h = e(P, Q)$, where $e : G_1 \times G_1 \rightarrow G_t$ then $h = g^a$ through bilinearity. Now, if one has an efficient algorithm to compute the discrete logarithm of $h \in G_t$, one will discover a, the result of computing the elliptic curve discrete logarithm of $Q \in G_1$.[178] Thus, powerful algorithms to compute the discrete logarithm

[176] *Id.*

[177] Menezes, A.J., Okamoto, T., Vanstone, S.A. "Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field." *IEEE Transactions on Information Theory*, vol. 39, pp. 1639-1646. Sept. 1993.

[178] *Id.*

in finite fields can significantly reduce the security associated with curves that are not carefully chosen. Once curves have been selected, cryptosystems may be built from the Bilinear Diffie-Hellman Assumption.

Bilinear Diffie-Hellman Assumption (BDH): Let G_1 have prime order q and $e : G_1 \times G_1 \rightarrow G_t$ be an admissible pairing. Let P be a generator of G_1 and $a, b, c \in \mathbb{Z}_q^*$. Given any PPT algorithm A:

$$Pr[A(P, aP, bP, cP) = e(P, P)^{abc}] \leq \epsilon$$

where ϵ is negligible.

In summary, under the BDH assumption, one assumes the intractability of computing $k = e(P, P)^{abc}$ from (P, aP, bP, cP). Under this assumption, one can construct an encryption scheme that mirrors the method by which the Diffie-Hellman key exchange enables the El Gamal cryptosystem in finite fields. In fact, the Boneh-Franklin IBE protocol invokes the essence of tripartite key exchange designed by Joux.[179] Utilizing a variant of the Joux exchange and the IBE framework posed by Shamir, Boneh and Franklin were able to construct the first functional, efficient IBE scheme. The following is an illustration of the Boneh-Franklin IBE protocol.[180]

[179] Joux, A. "A One Round Protocol for Tripartite Diffie-Hellman." *Proceedings of the Fourth Algorithmic Number Theory Symposium,* Lecture Notes in Computer Science, vol. 1838, pp. 385-394. 2000.

[180] Boneh, D., Franklin, M. "Identity-Based Encryption from the Weil Pairing." *SIAM Journal of Computing,* vol. 32, No. 3, pp. 586–615. 2003.

4.1.2 Boneh-Franklin Identity-Based Encryption

1. `Setup`(λ) : Perform the following:

   (a) Generate two groups G_1 and G_2 of prime order q, select admissible BDH bilinear map $e : G_1 \times G_1 \to G_2$, and choose generator $P \in G_1$

   (b) Choose a random $s \in \mathbb{Z}_q^*$ and initialize the public parameter $P_{pub} = s \cdot P$

   (c) Initialize the hash functions:

   $$H_1 : \{0,1\}^* \to G_1$$

   $$H_2 : G_2 \to \{0,1\}^n$$

   for some n

2. `Extract`(s, ID) : Compute $pk_{ID} = s \cdot H_1(ID)$

3. `Encrypt`(ID, m) : With some message $m \in \{0,1\}^n$, sample random $r \in \mathbb{Z}_q^*$. Compute the ciphertext

   $$c = (c_1, c_2) = (r \cdot P, m \oplus H_2(e(H_1(ID), P_{pub})^r))$$

4. `Decrypt`(c, pk_{ID}) : Compute $m' = c_2 \oplus H_2(e(pk_{ID}, c_1))$

For correctness, observe:

$$\begin{aligned}
m' &= c_2 \oplus H_2(e(pk_{ID}, c_1)) \\
&= m \oplus H_2(e(H_1(ID), P_{pub})^r) \oplus H_2(e(pk_{ID}, r \cdot P)) \\
&= m \oplus H_2(e(H_1(ID), s \cdot P)^r) \oplus H_2(e(s \cdot H_1(ID), r \cdot P)) \\
&= m \oplus H_2(e(H_1(ID), P)^{s \cdot r}) \oplus H_2(e(H_1(ID), P)^{s \cdot r}) \\
&= m
\end{aligned}$$

In summary, the above obtains IND-ID-CPA, as demonstrated in the original Boneh-Franklin paper, but the above is not IND-ID-CCA secure. An adversary may modify the ciphertext in transit and generate a valid plaintext. For instance, an adversary may take ciphertext:

$$c = (c_1, c_2) = (r \cdot P, m \oplus H_2(e(H_1(ID), P_{pub})^r))$$

and modify the message with some m' as follows:

$$c' = (c_1, m' \oplus c_2) = (r \cdot P, m' \oplus m \oplus H_2(e(H_1(ID), P_{pub})^r))$$

Thus, to win the above IND-ID-CCA game, an adversary performs the following:

1. Send the challenger the following messages: $m_0 = 0^n$ and $m_1 = 1^n$
2. Ask for the challenge encryption $c = (c_1, c_2)$ for some ID^* and m_b for random $b \leftarrow \{0, 1\}$
3. Query $\mathcal{O}^{ID,c}$ on ciphertext $c' = (c_1, 1^n \oplus c_2)$
4. If the response to the query $m' = 1^n$ then output $b' = 0$. Else, output $b' = 1$

In summary, the adversary takes advantage of the homomorphism in the second entry within $c = (c_1, c_2)$. As a result, Boneh and Franklin construct the following IND-ID-CCA variant of the above:[181]

1. `Setup`(λ) : Perform the following:

   (a) Generate two groups G_1 and G_2 of prime order q, select admissible BDH bilinear map $e : G_1 \times G_1 \to G_2$, and choose generator $P \in G_1$

   (b) Choose a random $s \in \mathbb{Z}_q^*$ and initialize the public parameter $P_{pub} = s \cdot P$

   (c) Initialize the hash functions:

   $$\begin{aligned} &H_1 : \{0,1\}^* \to G_1 \\ &H_2 : G_2 \to \{0,1\}^n \\ &H_3 : \{0,1\}^n \times \{0,1\}^n \to \mathbb{Z}_q^* \\ &H_4 : \{0,1\}^n \to \{0,1\}^n \end{aligned}$$

   for some n

2. `Extract`(s, ID) : Compute $pk_{ID} = s \cdot H_1(ID)$

3. `Encrypt`(ID, m) : With some message $m \in \{0,1\}^n$, sample random $\sigma \leftarrow \{0,1\}^n$, compute $r = H_3(\sigma, m)$, and generate the ciphertext:

   $$c = (c_1, c_2, c_3) = (r \cdot P, \sigma \oplus H_2(e(H_1(ID), P_{pub})^r), m \oplus H_4(\sigma))$$

4. `Decrypt`(c, pk_{ID}) : Compute the following:

   (a) $\sigma = c_2 \oplus H_2(e(pk_{ID}, c_1))$

[181] *Id.*

(b) $m = c_3 \oplus H_4(\sigma)$

(c) $r = H_3(\sigma, m)$

- If $c_1 \neq r \cdot P$, output $\perp$
- Else, accept ciphertext

Here, c_3 ensures that the homomorphism permitted by c_2 cannot yield valid ciphertexts. In other words, if an adversary were to play the same strategy in the IND-ID-CCA game above, an invalid ciphertext would be generated, and `Decrypt`$(\cdot)$ performed by the challenger would output $\perp$.

Note, the security of the Boneh-Franklin protocol relies on the intractability of recovering the master secret s from $P_{pub} = s \cdot P$, as well as the BDH assumption. Further, security relies on the assumption that $H_1(\cdot)$ and $H_2(\cdot)$ behave like random oracles. If the $H_1(\cdot)$ is not collision resistant, then multiple IDs may generate the same private key. Moreover, if $H_2(\cdot)$ is not collision resistant, the entropy of the cipher decreases in proportion to the lack of collision resistance. In any event, if s were efficiently computable, an adversary could compute the private key for any ID, effectively simulating extraction performed by the PKG. Authentication of the message upon receipt is not addressed in the above.

4.2 Kerberos

Kerberos enables clients and servers to mutually authenticate over an insecure network with shared resources.[182] In total, there are three entities involved in an authentication

[182] Neuman, C., Ts'o, T. "Kerberos: An Authentication Service for Computer Networks." *IEEE Communications Magazine*. pp. 33-38. Sept. 1994. Also, see: https://web.mit.edu/kerberos/papers.html.

instance: the authentication server (AS), which stores all user passwords and the passwords of all services; the ticket-granting server (TGS), which grants tickets for services on the network; and the services server (SS), which provides the service of interest. To begin, every client creates a password with the AS. To gain access to the system, the client sends its ID to the AS in plaintext. After receiving the ID, the AS looks for the password that corresponds to the ID in its database. If the ID is found, the AS generates a key k from the password and sends back the following:

{TGS session key} - encrypted with the client's secret key k

{ID | network address | expiration | TGS session key} - encrypted with TGS's secret key

The client attempts to decrypt the first message using its secret key to obtain the TGS session key, storing the second message as a ticket-granting ticket. If decryption is successful, the client sends the following to the TGS:

{ID | network address | expiration | TGS session key} - encrypted with TGS's secret key

{ID | network address | timestamp} - encrypted with TGS session key

The TGS decrypts the first message in oder to obtain the TGS session key. Next, the TGS uses the TGS session key to decrypt the second message and subsequently verify the ID of the sender, ensuring that the timestamp is before the stated expiration. If all is successful, the TGS transmits the following to the client:

{ID | network address | expiration | service session key} - encrypted with service server's key

{server session key} - encrypted with the TGS session key

After receiving the above, the client decrypts the second message to obtain the server session key and transmits the following to the SS:

{ID | network address | expiration | service session key} - encrypted with service server's key

{ID | network address | timestamp} - encrypted with the service session key

Lastly, the SS decrypts the first message to obtain the server session key. Then the SS decrypts the second message to verify the identity of the sender and to ensure that the lifetime of the ticket has not expired. The client and SS can now exchange information using the service session key.

Note, there is a single point of failure in the AS, which stores the keys for every client and the TGS. Further, the protocol involves a relatively high number of exchanges which may not be suitable for every context. Notably, the protocol only requires each user to authenticate once in order to avail of all services on the system for a limited amount of time. For instance, after the client provides the AS with its password and obtains a ticket-granting ticket, the client may obtain tickets for services until the ticket-granting ticket expires.

4.3 Prior Work

This study builds on advances in key management for identity-based encryption protocols. There exists forms of authenticated, or certificateless identity-based encryption. However, some do not use a distinct trusted third party for authentication, instead relying on the ability to prove possession of a valid private key from the same PKG in zero knowledge. There also exists approaches to removing the inherent escrow, but these protocols require additional interaction beyond a single transmission or do not incorporate third party authentication.

Lynn presents an authenticated version of the Boneh-Franklin protocol.[183] In this approach, Lynn replaces the encryption and decryption algorithms in Boneh-Franklin with functions to ensure the integrity and authenticity of the ciphertext: `Authenticated-Encrypt` and `Authenticated-Decrypt`. `Authenticated-Encrypt` generates an extra ciphertext element which is used to verify the integrity of the message within `Authenticated-Decrypt`. While this approach verifies the authenticity of the message, the protocol does not incorporate a distinct third party for authentication. The result is a PKG which retains an escrow into all encryptions. Moreover, parties must trust the same PKG for authentication to proceed successfully.

Others present certificateless schemes which include verification of ciphertext integrity but remove the PKG escrow. For instance, Al-Riyami and Paterson present a system with key generation algorithms to be performed by the PKG as well as each node in the system.[184] The resultant protocol – although without identity-based public keys – allows each node to prove knowledge of the system secret and to encrypt messages without a PKG escrow. Chow also presents an approach to eliminate the escrow and to provide the same authenticity as the Lynn and Al-Ryami and Paterson. Here, the user chooses an identity, obtains certification for the identity from an Identity Certifying Authority (ICA), and subsequently presents the certificate to a Key Generation Center

[183] Lynn, B. “Authenticated Identity-Based Encryption.” Cryptology ePrint Archive, Report 2002/072. Jun. 3, 2002.

[184] Al-Riyami S.S., Paterson K.G. “Certificateless Public Key Cryptography.” *Advances in Cryptology - ASIACRYPT 2003.* Lecture Notes in Computer Science, vol. 2894. Berlin, Heidelberg: Springer, 2003.

(KGC) to receive a private key. In effect, the ICA first registers the identity through a digital signature; after which the KGC verifies ICA signature and issues a private key corresponding to a public key which remains known only to the ICA. Thus, if the KGC or master secret are compromised, ciphertexts remain indistinguishable between identities.[185] It remains unclear how much anonymous ciphertext indistinguishability (ACI-KGC) in Chow mitigates the effects of secret compromise, since an identity may become known through means other than KGC compromise.

However, the concept of utilizing a third party to verify identity-based encryption public keys – and the option to utilize a distinct security assumption – illustrated in Chow provides insight into methods for third party verification and credential management. For instance, Kiltz and Vahlis suggest an IBE protocol using symmetric key authentication. Here, the ciphertext is given an integrity-check, meaning an adversary cannot generate fraudulent ciphertexts which successfully pass decryption using the exchanged key.[186] However, there remains an escrow into communication via the PKG, and a method to authenticate the origin of the message is not addressed.

To address verification of identity-based, public-key credentials, IETF RFC 6539 presents the Identity-Based Authenticated Key Exchange (IBAKE). In IBAKE, two parties perform a mutually authenticated exchange of elliptic curve Diffie-Hellman public keys.[187] However, the protocol involves a three way key exchange for mutual authentication between parties which utilize the same PKG. Thus, initial verification of each party's public-key credentials is assumed. Depending on the environment, a three way key

[185] Chow S.S.M. "Removing Escrow from Identity-Based Encryption." *Public Key Cryptography – PKC 2009.* Lecture Notes in Computer Science, vol. 5443. Berlin, Heidelberg: Springer, 2009.

[186] Kiltz, E., Vahlis, Y. "CCA2 Secure IBE: Standard Model Efficiency through Authenticated Symmetric Encryption." Cryptology ePrint Archive, Report 2008/020. 2008.

[187] Cakulev, V., et al. "IBAKE: Identity-Based Authenticate Key Exchange." Internet Engineering Task Force, Independent Submission, Request for Comments: 6539. Mar. 2012. https://tools.ietf.org/html/rfc6539#section-3.1.

exchange may exceed certain constraints. Further, the initiating party requires knowledge of the responding party's public key before the exchange, possibly requiring at least minimal key predistribution or an increase in the number of interactions.

4.4 Kerberized Identity-Based Encryption (KIBE)

Identity-based encryption delivers opportunities for key management that limit requirements for key distribution, allow administrators to audit nodes within a given system, and facilitate forward secrecy. However, current protocols to authenticate identity-based credentials often require sending and receiving parties to be in the same system. Further, existing mechanisms do not explicitly demonstrate how parties within distinct systems can utilize a trusted third party – which is not either of the systems' PKG, inherently possessing an inherent escrow – and symmetric key encryption to mutually authenticate communicating parties. This thesis's protocol, Kerberized Identity-Based Encryption (KIBE) suggests an identity-based credential management protocol which employs a trusted entity to authenticate nodes between distinct systems. Each system, operating under a distinct PKG, will have an escrow into system nodes. However, the trusted third party will not have an escrow into any communication, serving only as a mechanism for authentication. Further, KIBE allows parties to encapsulate a key, encrypt a message, and verify the authenticity of the aforementioned in a single transmission with minimal key predistribution.

Assume $\mathcal{S}_i = \{id_i^1, ..., id_i^n\}$ is the set of identifiers under the purview of the PKG of a given system, $\mathcal{S}_i$. Further, assume $Enc^1_{id_i^\alpha, \mathcal{P}_i}(\cdot)$ is the Boneh-Franklin encryption algorithm for some identifier id_i^α and $Dec^1_{pk_{id_i^\alpha}, \mathcal{P}_i}(\cdot)$ is the corresponding decryption algorithm.

In addition, let $Enc^2_k(\cdot)$ be a symmetric key encryption algorithm for key $k \in \{0,1\}^*$ and $Dec^2_k(\cdot)$ be the corresponding decryption algorithm. Without loss of generality, the following phases define the KIBE protocol for a message exchange between two nodes, id^α_i and id^β_j, under distinct PKGs:

1. `Registration`(λ) : Each PKG registers its $\mathcal{S}_i$ with the Key Management Center (KMC), where λ is the KMC security parameter. Registration involves establishing a shared symmetric key $k_{id^\alpha_i} \in \{0,1\}^\lambda$ between all $id^\alpha_i \in \mathcal{S}_i$ and the KMC. Further, each PKG provides the KMC with Token expiration information, t_i, and the public parameters $\mathcal{P}_i$ for its identity-based encryption system.

2. `Gen_Cert`$(id^\alpha_i, id^\beta_j, k_{id^\alpha_i}, \mathcal{P}_j)$: The KMC uniformly at random chooses $v \leftarrow \{0,1\}^\lambda$ and generates certificate:

$$\mathcal{C} = Enc^2_{k_{id^\alpha_i}}(id^\beta_j | t_j | \mathcal{P}_j | v)$$

3. `Gen_Token`$(id^\alpha_i, id^\beta_j, k_{id^\beta_j}, v)$: The KMC generates the following Token:

$$\mathcal{T} = Enc^2_{k_{id^\beta_j}}(id^\alpha_i | v)$$

   and sends $(\mathcal{C}, \mathcal{T})$ to id^α_i

4. `Encrypt`$(\mathcal{C}, \mathcal{T})$: Node id^α_i generates session key $k_s \leftarrow \{0,1\}^*$ and jointly encapsulates the session key and v:

$$(c_1, c_2) = Enc^1_{id^\beta_i, \mathcal{P}_i}(k_s | v)$$

   Now, id^α_i encrypts message $m \in \{0,1\}^*$ to generate ciphertext:

$$c_3 = Enc^2_{k_s}(m)$$

Lastly, id^α_i sends the following Message Packet to id^β_j :

$$\mathcal{M} = \{c_1, c_2, c_3, \mathcal{T}\}$$

5. `Decrypt`$(\mathcal{M}, pk_{id^\beta_j})$: Node id^β_i executes the following:

   (a) $k_s, v' \leftarrow Dec^1_{pk_{id^\beta_i}, \mathcal{P}_i}(c_1, c_2)$

   (b) $id^\alpha_i, v'' \leftarrow Dec^2_{k_{id^\beta_j}}(\mathcal{T})$

   (c) If $v' \neq v''$, output $\perp$

   (d) Else, output $m = Dec^2_{k_s}(c_3)$

In summary, one party receives a certificate and a token from the KMC, decrypts the token, and uses its contents to share a session key with the second party. The second party is able to authenticate the first party through decrypting the token, which the first party sends with the encapsulated key and encrypted message. Correctness follows from the Boneh-Franklin IBE protocol and the chosen symmetric encryption algorithm.

Security

First, note from above that the Boneh-Franklin protocol is minimally IND-ID-CPA secure in the random oracle model. Moreover, the IND-ID-CCA variant could easily be implemented, sacrificing the additional bandwidth required for larger ciphertexts – see Figure 5 for ciphertext expansion. In addition, the Kerberos-type certification delivers authenticity to the protocol, under the assumed intractability of inverting $Enc^2_k(\cdot)$.

Notice the incorporation of verification string $v \in \{0,1\}^\lambda$ provided by the KMC and encapsulated with the session key k_s prevents an adversary from relaying the token before the intended party can send a permissible message. However, v may also ensure that ill-formed ciphertexts cannot decrypt successfully. For instance, the concatenation operation performed by the id_i^α to encapsulate the session key and verification string may alternatively be the xor:

$$(c_1, c_2) = Enc^1_{id_i^\beta, \mathcal{P}_i}(k_s \oplus v)$$

Now, even if the IND-ID-CPA Boneh-Franklin protocol is utilized, reserving some bandwidth, KIBE may achieve IND-ID-CCA security through incorporation of the token for authenticity. Here, even if an adversary is able to efficiently invert the Boneh-Franklin encryption algorithm, $Enc^1(\cdot)$, KIBE still protects both the session key and the verification string, based on the same argument for OTP security mentioned previously. Therefore, producing ill-formed ciphertexts and winning the IND-ID-CCA game reduces to the hardness of inverting the OTP. Nonetheless, if the trusted third-party is able to break $Enc^1(\cdot)$, the party will be able to compute the session key and obtain an escrow into cross-constellation communication, beyond the simple escrow that may be present for intra-constellation communication provided by the IBE PKG.

Implementation

KIBE was implemented on a cluster of small computers operating within a closed network. The computers are networked to be able to communicate directly with one another. In implementation, the IND-ID-CPA Boneh-Franklin protocol was utilized; however, without loss of generality, any permissible IBE approach could be employed.

Further, AES-GCM was employed for all symmetric encryption, generating ciphertext and a tag for integrity and authenticity verification.

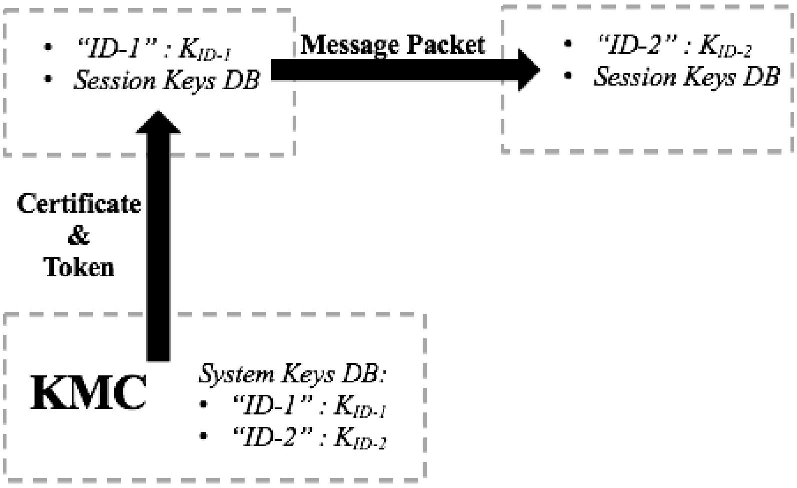


Figure 2: KIBE flow of information in a two-party example.

Figure 2 illustrates the general flow of information during an initial message exchange. During `Registration`, each computer submits a user-specified identity and generates a random 32-byte symmetric key to share with the KMC – a chosen computer on the system. Each computer additionally submits the public parameters used for its IBE system. This process simulates a satellite constellation operator, acting as a PKG for his system, cryptographically registering the constellation with some KMC.

At this point, the KMC stores the identities, public parameters, and unique symmetric keys associated with each of the satellites that have been registered. Now, the KMC may distribute certificates and tokens to chosen nodes. In implementation, a 16-byte verification string was used; although, if the encapsulation algorithm connects the verification string and session key through the xor operation, the verification string would need to be at least the size of the session key, requiring standardization of session key sizes or an agreement to utilize some fraction of the verification string. Upon receipt of a token-certificate pair, a node may establish a secure channel to communicate with the node for which it has been delivered a token. Until then, tokens and the information unpacked from within the corresponding certificate are stored in database on each computer.

To communicate directly between computers – simulating cross-link communication between two distinct constellations which have been registered with the KMC – a node sends a message packet to the desired node on the system. In implementation, the initiating node knows that the responding node exists since it has received a token to communicate with the responder. Moreover, communication between any two nodes is permitted on the network. In practice, for cross-link communication, there will likely have to be an established mechanism to establish sufficient situational awareness so that initiating satellites know which direction to orient a broadcast to a responder. Nevertheless, after the initial transmission, communicating parties will have established a shared symmetric key for future communication, storing such keys in a local database. Moreover, when new parties are added to the system, nothing needs to change. The new party registers with the KMC, and the KMC issues certificate-token pairs to the new party for authenticated communication with any existing node.

As a performance enhancement for users, may execute database queries to their node – which may be thought of as a satellite – to determine which entities the node has established a shared key with and for which entities the trusted third-party has provided a token for authentication. Note, the above allows two different satellite operators to submit unique IBE approaches for use. For instance, one party may wish to use a larger elliptic curve security parameter to receive a session key. So long as initiators are willing to encrypt with the specified security parameter, sufficient information to do so is provided by the certificate delivered by the KMC.

Extensions

One can implement KIBE with any identity-based encryption algorithm. If attacks against elliptic curve, or pairing-based cryptography become more sophisticated, one may utilize a different IBE protocol with a stronger security assumption. For instance, Gentry, Peikert, and Vaikuntanathan (GPV) have demonstrated an identity-based protocol which relies on the assumed hardness of the learning with errors problem, which may hold potential resistance against quantum adversaries.[188] It is also possible to implement a variant of KIBE using any form of public-key cryptography, but credential management may become more cumbersome for forward secrecy without an identity-based mechanism. Additionally, each PKG will not necessarily have an escrow into its nodes' communication for auditing.

Further, in some cases, one may want to ensure that the token, $\mathcal{T}$, and certificate, $\mathcal{C}$ are inherently linked. To do so, one may hash, $H(\cdot)$, the token and include the hash within the certificate, as follows:

$$\mathcal{C} = Enc^2_{k_{id_i^\alpha}}(id_j^\beta|t_j|\mathcal{P}_j|v|H(\mathcal{T}))$$

Then, the KMC proceeds as normally to send $(\mathcal{C}, \mathcal{T})$. Further, after decryption of the certificate, the recipient verifies the hash of the token.

Ultimately, KIBE jointly employs symmetric and asymmetric cryptography to enable parties to communicate a single transmission which establishes a shared key, exchanges

[188] Gentry, C., Peikert, C., Vaikuntanathan, V. "How to Use a Short Basis: Trapdoors for Hard Lattices and New Cryptographic Constructions." *Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing.* pp. 197-206. 2008.

an encrypted message, and provides a tool for authentication. On the downside, KIBE requires significant time to encrypt messages – see Figure 3. Moreover, authentication, whose latency may mitigate denial of service attacks, requires decryption using the employed IBE mechanism. Thus, asymmetric cryptography is utilized for authentication, affecting the overall latency of decryption – see Figure 4. As a result, KIBE would benefit from faster pairing algorithms or more computationally efficient IBE algorithms. Nonetheless, distinct security assumptions, especially if the session key and verification string are combined using the xor operation within the IBE encryption algorithm, support strong confidentiality and authenticity.

Moving forward, and in practice, satellites will require a means to direct broadcasts in the correct direction toward destinations of interest. Although satellites of different constellations do not need overlapping cryptographic material, and key predistribution is not required for cross-constellation communication, KIBE requires some amount of key distribution, in the form of tokens and certificates, which may become too burdensome for some applications. Under KIBE, one can parameterize the lifetime of certificate-token pairs through effective time-stamping, but decreasing the lifetime of such tools increases the complexity in key distribution, and increasing the lifetime disables flexible key revocation. Ultimately, KIBE balances symmetric and asymmetric authentication, with minimal key distribution.

Complexity Results

The below were tested using a 2 GHz Intel Core i7 processor. Note, computation time may vary depending on the specific hardware utilized, but the relative differences between speeds associated with different security parameters may remain. Further, the time complexity of the IND-ID-CPA and IND-ID-CCA Boneh-Franklin protocols are nearly identical, and only the IND-ID-CPA version is displayed for clarity.

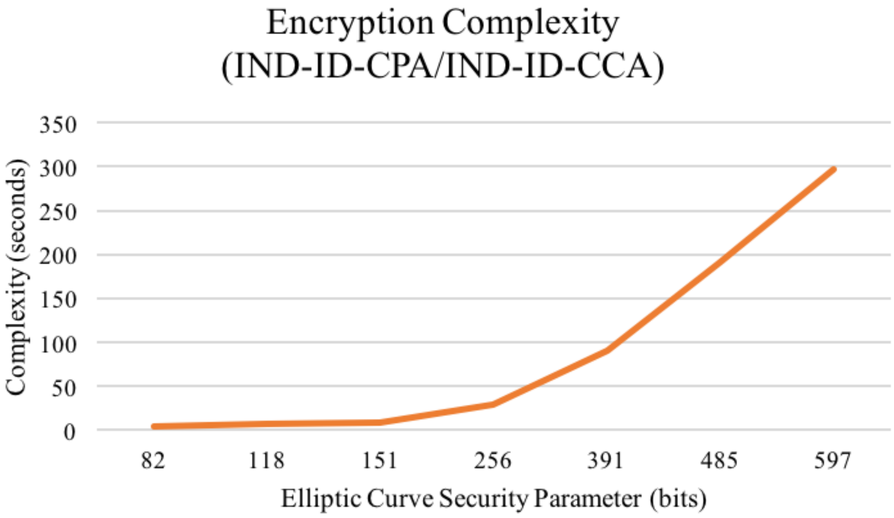


Figure 3: Time complexity of encryption for implementation of Boneh-Franklin using the Tate pairing, given a security parameter for the elliptic curve.

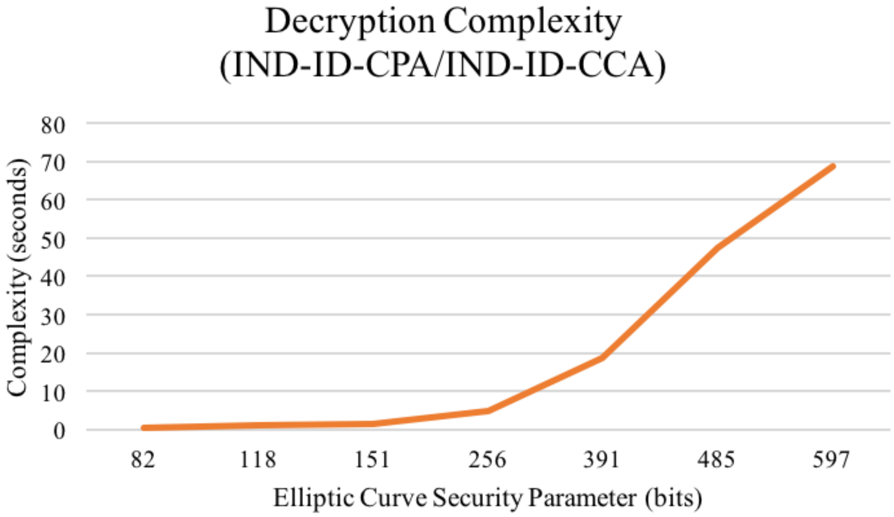


Figure 4: Time complexity of decryption for implementation of Boneh-Franklin using the Tate pairing, given a security parameter for the elliptic curve.

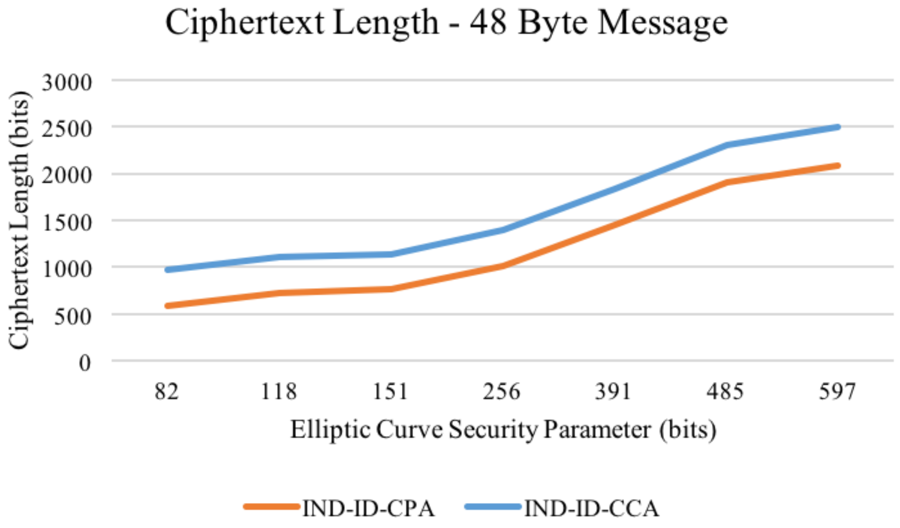


Figure 5: Ciphertext length in bits for implementation of IND-ID-CPA and IND-ID-CCA Boneh-Franklin using the Tate pairing, given a security parameter for the elliptic curve. Message in $\{0,1\}^{256}$ and Verification String in $\{0,1\}^{128}$.

Conclusion

Ultimately, while the encryption and decryption algorithms perform a single pairing operation, encryption performs two point addition operations over the elliptic curve while decryption does not perform any. Moreover, the IND-ID-CCA protocol contains roughly 48 additional bytes to account for the third component ciphertext, which is the length of the message concatenated with the verification string.

It remains to be shown what entity will embody the KMC. In the above implementation, all computers – and hence satellite operators – trust the chosen computer which acted as the KMC. Next, this study addresses which actors may act as the trusted third-party for cross-constellation communication between assets which deliver international services and may operate according to distinct national jurisdictions.

5 A System for Registration

A network of registration mechanisms which coordinate instruments for cryptographic authentication between state and non-state actors may allow disparate constellations to protect communication between one another. The groups which participate in such registration, which already intend to communicate, may also engage in cooperative agreements to off-load traffic in the event that any particular satellite constellation sustains a system upset. Indirectly, this may allow state and non-state actors to deploy fewer assets to orbit, easing concerns pursuant to the Outer Space Treaty and its supporting instruments. KIBE, or another protocol, may address credible establishment of shared cryptographic material, and the registration mechanisms could act as trusted third-parties to verify the authenticity of credentials external to one's system. This new registration system, with whatever party, is simply a means to authenticate communication across distinct constellations for variable periods of time. Although, the consequences of such a system imply the possibility of robust cooperation like that observed between submarine cables, promoting the responsible, sustainable use of the domain.

As noted, the Registration Convention already requires each state to inform the UN about the launch and function of any space objects under the state's purview.[189] Currently, the Registration Convention itemizes information which must be submitted to the UN's space object registry, and while this information does not always support the most specificity, the system illustrates that states are amenable and accustomed to registering their assets with an international body.[190] Further, if the UN maintains an interest in regulating the behavior of actors in outer space, and if those interests seek to encourage

[189] *Supra* note 107.

[190] For comments on material often submitted during registration, see: *supra* note 109.

constellation interoperability, then the body may also aim to ensure that assets are able to locate trusted third-parties for inter-constellation authentication. In the end, there are three broad roles for UN participation in a regime of authenticated communication in outer space, which are listed in increasing order of viability: 1) act as the sole key management center for authentication through a functional agency; 2) certify the use of existing commercial certificate authorities; and 3) encourage, and possibly guide through treaty instruments, the formation of consortiums which support their own infrastructure, as is the case in the undersea cable community. The balance of this section illustrates the three options and argues that the third option is the most practical, appropriate option for cross-constellation authentication, and further, suggests that UN instruments could facilitate their formation through instruments which encourage actors to limit the number of assets deployed to deliver a particular service.

1. Single International Certificate Authority

In practice, a functional agency under UN, such as the ITU or an agency which consults with the UN such as the International Organization for Standardization (ISO), could position itself to act as a trusted third-party for authentication. In this regime, each satellite operator would submit the necessary cryptographic material to the body such that the body can derive KIBE, or other, certificates and tokens for cross-constellation authentication. This would not be too dissimilar from existing registration with the ITU, but storage of cryptographic material in a single location may present a high-degree of risk. Moreover, attempts by the UN-affiliated body to enforce treaty instruments – such as through key revocation – may preclude initial participation, given that states likely do not want to abdicate control of certain networks to a single body and may dispute the bar above which provisions may be asserted. Although, a critical benefit of this system may be the use of shared terrestrial gateways, promoting a degree of standardization which may later facilitate interoperability and advance measures to alleviate concerns pursuant to the Outer Space Treaty.

There are two key differences between the provisions within the Constitution and Convention of the ITU and those asserted by the Registration Convention. The first, which is a necessary condition of the second, relates to specificity. The ITU has registration process which requires a detailed account of the frequency bands which actors intend to consume. Thus, actors know exactly what data to submit, and such information is not only sufficient, but also constant across borders. Moreover, the narrowness of the required information does not force actors to additionally submit information which they may deem unnecessary, such as function or identification of any particular satellite.[191]

Second, the aforementioned specificity subsequently enables states to enact legislation which corresponds, nearly exactly, to the international framework. For instance, in the U.S., 47 CFR §25.111 directs the FCC to register frequency assignments with the ITU on behalf of commercial entities. Further, the federal code asserts that "[n]o protection from interference caused by radio stations authorized by other [actors] is guaranteed unless ITU procedures are timely completed."[192] In sum, due to a well-acknowledged, collective benefit through this form of registration, as well as a detailed account of the information required, actors are willing to register and state instruments can mirror international frameworks in order to enforce directives therein.

[191] *Supra* note 112. Note it is possible that the dearth of satellites deployed does not promote the value of satellite identification, since the instances where such knowledge is required may be limited. However, as the number of assets in orbit grows, so too may the importance of this item within the Registration Convention.

[192] 47 CFR §25.111(b).

Even with explicit language for cryptographic registration with a central body, security is likely the primary factor to justify a different approach to an international infrastructure for third-party authentication. If a single body contains cryptographic material to authenticate every satellite which chooses to participate in the system, there exists a significant point of failure and one probably does not deliver individual actors a large influence over how the system operates. Further, there likely will not exist any *legal* instruments to ensure that spacecraft adhere to this modality of authentication. Hypothetically, the functional institution storing the tools for authentication may revoke a constellation's privileges in order to enforce the laws set forth by the UN, but this may require constellations to sacrifice an element of sovereignty and will likely chill initial interest in the system.

However, this approach to over the air authentication delivers a useful feature which may translate to any apparatus aimed at accomplishing the same. Namely, any third-party system which is to communicate with all satellites must support all wavelengths at which space-based systems transmit up- and down-link communications. Moreover, this it not as unreasonable of an assumption at it seems *prima facie*. Existing systems, such as the Battlefield Airborne Communications Node (BACN), already obtain similar utility in aircraft. In practice, BACN nodes are flown above an operational zone where line of sight has been removed between assets on the ground and other communication infrastructures.[193] In addition, BACN systems are capable of digesting a received signal and replaying the same message at a disparate frequency, acting as a gateway between otherwise incompatible systems.[194] The entity managing authentication credentials could

[193] Dubois, K. "BACN Improves Communication for Deployed Troops." U.S. Air Force publication. Nov. 27, 2018. https://www.af.mil/News/Article-Display/Article/1698903/bacn-improves-communication-for-deployed-troops/.

[194] Manchenton, M. "Airborne Network Gateway Keeps Warfighters on the Same Wavelength." MITRE Project Stories. Feb. 2012. https://www.mitre.org/publications/project-stories/airborne-network-

do the same for all constellations through facilities operated solely by the body.[195]

Alternatively, the registry could route information through existing terrestrial infrastructures to the appropriate bodies in order to up-link the transmission to a given constellation. However, this approach presents a trade-off between the amount information each satellite stores and increase latency associated with authentication. It may be possible for the UN body, for instance, to issue KIBE tokens and certificates to satellites constellations periodically, depending on their expiration. Here, each satellite would have to dedicate storage for a repository of valid tokens and certificates, even if the satellite may never use them. Thus, the UN body may distribute cryptographic material unnecessarily, decreasing control over the information and presenting an additional challenge: namely, if a satellite is compromised the satellite may be able to authenticate itself to any number of trusted satellites. To avoid this form of predistribution, the UN body could issue certificates and tokens as needed at a cost in latency, since the flow of communication has to incorporate extra links between the body which generates the tokens and the entity which transmits information to any of the constellations.

Ultimately, KIBE and other over the air authentication protocols may benefit from commonly used gateways, but a network of BACN-like ground-based systems is likely most suited to be a commercial enterprise, similar to landing stations in the realm of undersea cables. Intergovernmental organizations (IGO) may practically fill the same role, but outer space IGOs with commercial application, such as INTELSAT and INMARSAT,

gateway-keeps-warfighters-on-the-same-wavelength.

[195] It's also easy to conceive of such a gateway in LEO. Satellites could exclusively operate as BACN-like gateways; there may develop a market for entities to deploy space-based gateways which move one frequency to another. Alternatively, two entities who do not normally utilize the same frequency but wish to create external redundancy may simply incorporate antennae on their buses for the dedicated purpose of assisting one another. Even more deeply, two constellations who are willing to assist one another in this way may also share frequencies within one another's FCC allotted bandwidth, providing each an opportunity to adaptively hop between frequency bands to suit a particular context. More discussion regarding the aforementioned can be found in the proceeding section covering the consortium-based approach to cross-constellation authentication.

are likely to fall under pressure to commercialize if existing systems in the private sector can perform the same function.[196] As noted, reduced costs allow commercial entities to enter the domain, and it is neither inconceivable nor technically prohibitive to imagine existing and future commercial gateways, at the very least, communicating with satellites of disparate constellations.

In the end, while this system appeals to collective benefit, it is unlikely that actors will abdicate security and control of independent networks to a single, international organization. Further, this infrastructure is likely incapable of addressing the specific needs of small groups of actors, favoring the system which works for most parties. Nevertheless, the best feature one may extract from this type of apparatus is a system of commonly used terrestrial gateways which are operated by a body, or number of bodies, which participating actors presumably trust.

2. Commercial Certificate Authorities

Commercial certificate authorities may provide a market-driven means for autonomous – without human involvement – authentication over the air, as well as encourage the commercialization of common terrestrial gateways, but they likely cannot encourage the

[196] Agreement Establishing Interim Arrangements for a Global Commercial Communications Satellite System. Aug. 20, 1964, 514 U.N.T.S. 26; Convention on the International Maritime Satellite Organization (INMARSAT), Sept. 3, 1976, 1143 U.N.T.S. 105. INTELSAT demonstrated ambitions to privatize in 1998 when it released 5 of its satellites to start a new communications company – New Skies Satellites, which would was later acquired by SES in 2005. However, INTELSAT wasn't completely privatized until 2001 after the Open-market Reorganization for the Betterment of International Telecommunications Act (ORBIT Act, 2000) called for its privatization in the U.S.. Commercial actors, such as PanAmSat, criticized INTELSAT for enjoying an unfair competitive advantage as an intergovernmental institution and Congress agreed. United States Government Accountability Office, Report to Congressional Requesters. "Intelsat Privatization and the Implementation of the ORBIT Act." Sept. 2004. Blackstone press release. "SES Global to Aquire New Skies Satellites." Dec. 14, 2005. https://www.blackstone.com/media/press-releases/article/ses-global-to-acquire-new-skies-satellites. Inmarsat, in view of the New Skies break-off, privatized in the U.S. in 1999. Feder, B. "Satellite Company is Trying Life on its Own." *New York Times.* Jul. 23, 2001. McCormick, P. "The Demise of Intergovernmental Satellite Organisations." *Journal of International Communication.* May 3, 2011.

extent of cooperation observed in the undersea cable community, a feature which may enhance consistency among states' interpretations of UN-brokered instruments and compliance therein. Nonetheless, commercial vendors may adjust to changing security requirements and provide customers with tools to meet specific needs, remaining a viable certificate authority for space-based systems which may only need to be bolstered by an additional apparatus to facilitate broader constellation interoperability.

Commercial actors already authenticate communication between parties over a common network, suggesting that actors may be amenable to a continuation of the practice. For instance, Symantec, DigiCert, and others build public-key infrastructures (PKI) and execute third-party verification to support the authenticity of websites on the Internet. While existing PKI approaches may not currently account for the concerns with space-based assets that KIBE attempts to address, commercial actors could likely adapt and ultimately perform the service. However, the commercial system is likely to suffer from the same trade-off between storage and latency observed in the previous regime.

In addition, the UN does not have to be isolated from the authentication process, but its practical influence may vary. The UN, or a functional agency therein, could maintain a repository of recommended certificate authorities. Here, a specialized agency, such as the ISO, could actively publish a list of the certificate authorities which it believes to most optimally meet the challenges of outer space. Actors could then have an available, credible resource to assist in decision making. It is unlikely that actors would accept some standard set by the UN regarding which commercial authorities to utilize, but actors may continue to appreciate the advice of recognized bodies, such as the ISO and NIST.[197]

In sum, commercial tools for authentication are likely to adapt to provide meaningful security and deliver actors the ability to choose which authorities are permitted to au-

[197] *Supra* note 12.

thenticate their broadcasts. However, commercial authentication, isolated from broader cooperative efforts, may not encourage the extent of cooperation observed by undersea cables, thereby enhancing service resiliency and sustainability of the domain. Namely, agreements to off-load traffic in the event that a critical network asset is damaged require additional mechanisms beyond commercial authentication of communication. Ultimately, an infrastructure which balances the benefits of commercialization and the involvement of international instruments, such as those provided by functional agencies under the UN, may distribute security away from a single entity, deliver actors more agency over tools for authentication, and build an system that lowers the barrier to an interconnectedness which promotes a more consistent application of international legal instruments.

3. Consortiums of Satellite Operators

Small collections of actors, which negotiate under the availability and legitimacy of UN resources, can initiate cooperative groups based on common system features to not only coordinate tools for authentication, but also share terrestrial gateways and network resources, extracting the advantages of the previous two modalities. Notably, actors may reserve bandwidth over their channels for the event that a partner within their consortium needs to off-load traffic if a critical component becomes damaged. Thus, the consortium model, compared to certificate commercialization, may promote the broad cooperated offered by the single UN-affiliated body regime, but with the flexibility for groups of actors to choose to work together. Here, actors will have an opportunity to reduce individual costs at both initial deployment and after an event where an asset sustains damage – obviating the need to deploy in-orbit spares and to face situations like that handled by Panamsat.[198]

The UN could encourage actors, through non-binding resolutions, to join and form these consortiums, which by nature of operation inherently take steps to mitigate debris, continually supervise assets, and avoid "harmful contamination" of the domain.[199] However, the formation of such consortiums likely does not require UN involvement – so long as there are clear operational benefits to participation – and the aforementioned UN actions may exact little impact as non-binding instruments.

Alternatively, the UN may participate in the infrastructure through a more functional role. Namely, the UN could require that satellite operators demonstrate that they deploy the minimum assets necessary to deliver a particular service. This feature may require an additional treaty element, but if there exist standards by which states can encourage actors to initially limit the number of assets deployed, actors may be encouraged to join these types of consortium which inherently address several concerns associated with international law in the domain. The remainder of this study suggests a new registration process, supported by specific UN provisions which administer a minimum essential standard in order to address the interests of satellite operators and concerns pursuant to the Outer Space Treaty and its supporting instruments.

5.1 A Collection of Consortiums

Consortiums of satellite operators could collaborate on a suite of features for the advancement of their collective capabilities. Namely, members of each consortium could

[198] *Supra* notes 137-138.

[199] United Nations Treaty on the Principles Governing the Activities of States in the Exploration and Use of Outer Peace, including the Moon and Other Celestial Bodies, art. 9, Jan. 27, 1967, 610 U.N.T.S. 205.

cryptographically register each participating satellite with a key management center (KMC) operated by members within the consortium, and support the regular function of each participating constellation. The product may increase the persistence of each constellation's service and decrease the economic barrier to enter the market. This section first illustrates how entities may choose which constellations to partner with to form such consortiums, indicating that this is only possible through a high degree of physical and network standardization. Afterward, this section illustrates a possible modality for identity-based cryptographic registration and suggests that the formation of such consortiums may allow for tighter compliance with a consistent interpretation of existing international legal instruments. Moreover, this study illustrates that the UN, or a functional body such as the ITU, may encourage the formation of such consortiums by instituting provisions which close the numerical gap between the number of assets deployed and the number of assets required to deliver a service.

Actors which perform related or dependent services are the most positioned to practically work together. Undersea cable operators form their consortiums based on the regions they serve, but satellites operate over a much wider field. Even satellites which operate at different orbits may still be able to assist one another. For instance, satellites at low altitudes may passive amplify signals from satellites at higher altitudes, and satellites at lower altitudes, whose velocity exceeds that of the rotation of the Earth, may receive instructions from geosynchronous satellites as they pass through particular regions. Nonetheless, physical compatibility will determine which operators can enter into the same consortiums. Certain constellations with dedicated functions, like DSP and STSS, are unlikely to be able to allocate resources to assume the traffic of other constellations, since such action might inhibit their respective missions.

However, any satellites which host equipment to operate at the same frequency and coordinate network protocols may collaborate within each consortium. In doing so, each satellite will not require additional antennae to receive or repeat signals, eliminating size and weight concerns with equipment for interoperability. Notably, this requirement may already be practicable. When SpaceX requested to operate satellites within its Starlink constellation at a lower altitudes, OneWeb and Kepler, which plan to deploy similar constellations, filed petitions to the FCC in order to block the relocation.[200] OneWeb and Kepler argued that their constellations and Starlink operate at similar frequencies, thereby increasing the likelihood of interference.[201] Thus, if deleterious interference is a concern, then the satellites can likely communicate if they share similar electronic means for communication and network protocols.

Notably, SpaceX was also able to evade assertions that the likelihood of collisions with other space-based assets would increase should the assets change orbits, based on the argument that Starlink buses contain thrusters which can maneuver their satellites away from nearby objects.[202] However, a FCC Notice of Proposed Rulemaking asserts that there is "no requirement in the Commission's rules that space station licensees encrypt telemetry, tracking, and command communications," and notes that "small satellites, particularly those operated for academic purposes—may not use encryption for telemetry, tracking, and command communication links."[203] Thus, even if it were to be determined that one of the Starlink nodes is likely to collide with another object, communication to maneuver the assets may be forged. Far worse, information could be transmitted to

[200] The FCC ultimately did not accept these arguments and approved SpaceX's request to alter the altitudes of its future assets. Grush, L. "FCC Approves SpaceX's Plans to Fly Internet-beaming Satellites in a Lower Orbit." *The Verge.* Apr. 27, 2019.

[201] *Ibid.*

[202] *Ibid.*

[203] Federal Communications Commission Notice of Proposed Rulemaking and Order on Reconsideration, para. 74, Nov. 15, 2018.

increase the likelihood of a collision. Nevertheless, KIBE or another protocol would allow for the protected communication required to reliably relocate assets in the air.

Given sufficient physical and network interoperability satellite operators may form the previously mentioned consortium, but to reliably cooperate, even on tasks such as passive repeating, there must exist a transport security protocol to authenticate communication. In practice, this amounts to a shared approach to key management – for which the remainder of this paper uses KIBE for illustration. Under this model, each consortium could require that every satellite operator submit sufficient material to the trusted KMC in order generate KIBE certificate-token pairs for over the air authentication. Further, the KMC could be operated by personnel affiliated with each member constellation. These personnel would be required to handle the management of authentication credentials and administer registration. However, personnel operating the KMC are only permitted to deliver tools for authentication to each satellite on a basis which is dictated by the individual satellite operators, thereby limiting opportunities for malicious operators to compromise the KMC.

Using the identity-based approach espoused by KIBE, each satellite operator could register – with the consortium KMC – unique identifiers for each satellite within his constellation. The Registration Convention already asks for "an appropriate designator of the space object or its registration number,"[204] and this designator could serve as each satellite's public key and its international registration tag pursuant to the world registration phase. Next, each operator could extract a private key for each satellite using the appropriate identity-based cryptosystem, and deliver the associated public parameters and a shared symmetric key to the KMC. At this point, the KMC possesses the tools

[204] United Nations, Convention on the Registration of Objects Launched into Outer Space, art. 1, Sept. 15, 1976, 1023 U.N.T.S. 15.

necessary to construct KIBE tokens and certificates for any satellite in the consortium. Notably, the KMC will not be able to ascertain the semantics of any communication within or across constellations, under the design of KIBE.

Now, to preclude the relocation or reorientation of assets to make communication possible, inter-connected constellations could frequently transmit heartbeat signals to deliver a situational awareness update. Especially with respect to satellite in LEO, assets may constantly enter and exit the broadcast range of other satellites. Moreover, these heartbeat signals could comprise KIBE designators – their public keys – so that satellites within a consortium know which assets they are nearby and so that they may query the KMC for the tools for authentication. Thus, if one satellite stops responding, the system may automatically begin to reroute information without human intervention.

Further, the addition of satellites to the consortium is seamless. For instance, after a new asset enters the consortium, deployed satellites only need a KIBE certificate and token to communicate a protected message in a single transmission to the new asset. Moreover, revocation of access to the constellation is a function of the lifetime of KIBE tools, but may be parameterized based on KMC involvement. Namely, a KMC that wishes to be highly involved can issue KIBE certificates and tokens with short lifetimes, facilitating opportunities for key revocation, and a less involved KMC may issue longer-lasting tools with the opposite impact on credential revocation.

To further collaborate, each consortium could establish terrestrial gateways for common use among constituent constellations. Thus, the KMC could be paired with a network of trusted gateways, mitigating the storage to latency trade-off associated with the single UN-affiliated body and totally commercialized regimes. Note, while this may lower the economic barrier to enter the outer space market and increase the resiliency of each service, shared gateways are not necessarily a function that a consortium has to provide. In addition, commonly used gateways may create attractive points for adversaries to attempt to compromise, similar to the landing stations for undersea cables. Nevertheless, this approach may reduce the complexity of cryptographic coordination and certificate distribution for KIBE and other key management protocols.

It's worth noting, systems which require high-degrees of security, such as the DSCS constellation, may not engage in these types of consortiums since total agency over one's network may not be supported when off-loading traffic to another constellation. However, the telecommunications service offered by satellite systems such as DSCS may be replaced or utilized in parallel with the distributed options found in such consortiums. While information security may not meet certain requirements, the physical security and persistence of service offered by the these consortiums may be unmatched.

The formation of consotrium is likely not directly under the purview of the UN, but the consequences of their formation likely address provisions adopted by the UN General Assembly and widely ratified instruments. As a result, the UN may encourage their formation through provisions which lead entities to deploy the minimum number of assets necessary to deliver a service – a luxury which may be amenable to state and non-state parties if operators can rely on an infrastructure of connected satellites to support each constellation's individual service. As noted, deployment of space-based assets rests in both defense and public interests, but limiting the number of assets in orbit may help operators to satisfy provisions contained within Articles VI, VII, IX, and XI of the Outer Space Treaty. Notably, minimum essential standards and evolving as technology permits is not new to the field. The Constitution and Convention of the ITU asserts that "[m]embers shall endeavour to limit the number of frequencies and the spectrum used to the minimum essential to provide in a satisfactory manner the necessary services. To that end, they shall endeavour to apply the latest technical advances as soon as possible."[205] Moreover, as noted previously, the IADC has already espoused such a standard for the most effective debris mitigation programs.[206]

In practice, the UN, acting through the ITU, may adopt resolutions for state ratification which designate ITU reservation on the Master International Frequency Register (MIFR), which captures all of the allocated frequencies for international radiocommunications systems, if actors not only minimize the bandwidth required for their service but also minimize the number of physical assets required to deliver the service.[207] This would require legal instruments within each state to enforce such a provision, but the existing balance between states utilizing a sufficient, yet minimum necessary amount of bandwidth indicates practice in optimizing resource allocation for particular activities. The deployment of physical assets to a global domain could be viewed similarly.

If actors deploy less assets, they will diminish their responsibility to continually supervise their assets pursuant to Article VI. Further, less objects will need to be registered under Article XI and concerns with "potentially harmful interference" mentioned in Article IX will likely decline.[208] However, the largest benefit for states which choose to support the formation of the aforementioned consortium or some minimum essential standard may be observed with respect to Article VII: the risk of liability is likely limited if individual actors deploy fewer assets. Alternatively, if liability is ever transferred from states to commercial actors, as is the case under the 1884 Convention for the Protection

[205] Constitution and Convention of the International Telecommunication Union, para. 195, Oct. 1, 1994, 1825 U.N.T.S. 330.

[206] *Supra* note 91.

[207] *Id.* at para. 172

[208] United Nations Treaty on the Principles Governing the Activities of States in the Exploration and Use of Outer Peace, including the Moon and Other Celestial Bodies, art. 9, Jan. 27, 1967, 610 U.N.T.S. 205.

of Submarine Telegraph Cables, liability could be contractually distributed throughout entities within each consortium, essentially establishing an insurance program within the group.[209]

[209] *Supra* note 143.

6 Conclusion

While internationally recognized documents remain inconsistently interpreted, tenuously enforced, and neglect to promote constellation interdependence, debris will congest various altitudes and suppress the world's expectation for the future of space-based services. Independent of the functional role of the UN in authenticating cross-constellation communication, through active engagement with the topic, the UN could guide how actors approach and discuss authentication in other forums – just as the ill-fated League of Nations lead the charge toward facilitating international Through such guidance, the UN could advance objectives within the Outer Space Treaty, notably those related to Articles VI, VII, IX, and XII.

The consortium-based approach to over the air authentication and broader constellation interoperability is likely the most optimal mechanism to address both the interests of individual actors and political efforts directed at the sustainability of the domain. In this system, actors may exploit high degrees of compatibility to improve service resiliency, generate external redundancy, and establish an economy of assets that communicate to, transact with, and assist one another. The apparatus would be similar to that of undersea cable operations, but these consortiums may additionally acts as trusted third parties for cross-link communication. In the undersea cable model, endpoint users are required to support their own information security, allowing cable operators to focus on the availability of the system. This approach works in closed cables, but in an environment where broadcasts may be received from a variety of different sources, digital authentication is minimally required.

Regardless of the trusted third-party in cross-constellation authentication – the singular international certificate authority, commercial certificate authority, or the consortium approach – the same key management protocol could be employed to achieve confidentiality, integrity, and authenticity within the network. KIBE could be utilized by any group of actors which trust a KMC to deliver tools for authentication – a necessary element of any approach for protected communication between ephemerally trusting parties. Ultimately, the resultant infrastructure could enhance each independent service and increase the reliability of an international rule of law in outer space.

Bibliography

Aerospace Technology. “Globalstar Communication satellite.” https://www.aerospace-technology.com/projects/globalstar/. [132]

Agreement Establishing Interim Arrangements for a Global Commercial Communications Satellite System, Aug. 20, 1964, 514 U.N.T.S. 26. [196]

Al-Riyami S.S., Paterson K.G. “Certificateless Public Key Cryptography.” *Advances in Cryptology - ASIACRYPT 2003.* Lecture Notes in Computer Science, vol 2894. Berlin, Heidelberg: Springer, 2003. [184]

Berger, E. “Air Force Budget Reveals How Much SpaceX Undercuts Launch Prices.” *Ars Technica.* Jun. 15, 2017. [126]

Blackstone press release. “SES Global to Aquire New Skies Satellites.” Dec. 14, 2005. https://www.blackstone.com/media/press- releases/article/ses-global-to-acquire-new-skies-satellites. [196]

Bluecosmo. “Satellite Network Comparison Table.” https://www.bluecosmo.com/compare-satellite-networks. [134]

Boneh, D., Franklin, M. “Identity-Based Encryption from the Weil Pairing.” *SIAM Journal of Computing,* vol. 32, No. 3, pp. 586–615. 2003. [171,172,173,174,175,176, 180,181]

Cakulev, V., et al. “IBAKE: Identity-Based Authenticate Key Exchange.” Internet Engineering Task Force, Independent Submission, Request for Comments: 6539. Mar. 2012. https://tools.ietf.org/html/rfc6539#section-3.1 [187]

Caleb, H. “FCC Aproves SpaceX, Telesat, LeoSat, and Kepler Internet Constellations.” *Space News.* Nov. 15, 2018. [101]

Carter, A., Steinbruner, J., Zraket, C. *Managing Nuclear Operations.* Washington, D.C.: The Brookings Institution, 1987. [121]

Caughill, P. “Rocket Lab Has Successfully Launched its Electron Rocket Into Orbit.” *Futurism.* Jan. 23, 2018. [128]

Chappell, B. “NASA: Debris from India’s Anti-Satellite Test Raised Threat to Space Station.” *National Public Radio.* Apr. 2, 2019. [57]

Charter of the United Nations, Jun. 26, 1949. [5,68]

Coffey, V. “Sea Change: The Challenges Facing Submarine Optical Communications.” *The Optical Society: Optics and Photonics.* Mar. 2014. [158]

Cohen, Alexander F. "Cosmos 954 and the International Law of Satellite Accidents." *Yale Journal of International Law,* vol. 10, art. 7, 1984. [70,71,72]

Constitution and Convention of the International Telecommunication Union, Oct. 1, 1994, 1825 U.N.T.S. 330. [6,41,46,113,205]

Consultative Committee on Space Data Systems. "Space Missions Key Management Systems." Nov. 2011. https://public.ccsds.org/Pubs/350x6g1.pdf. [4,10,17,18,22,25]

Consultative Committee on Space Data Systems. "Symmetric Key Management." Jun. 2018. https://public.ccsds.org/Lists/CCSDS%203540R1/354x0r1.pdf. [9]

Convention on International Civil Aviation, Dec. 7, 1944. 61 Stat. 1180. [41]

Convention on the International Maritime Satellite Organization (INMARSAT), Sept. 3, 1976, 1143 U.N.T.S. 105. [196]

Cooper, N. "The Invisible Neutron Threat." Los Alamos National Laboratory: National Security Science. https://www.lanl.gov/science/NSS/issue1 2012/story4full.shtml. [129]

Chow, S.S.M. "Removing Escrow from Identity-Based Encryption." *Public Key Cryptography – PKC 2009.* Lecture Notes in Computer Science, vol. 5443. Berlin, Heidelberg: Springer, 2009. [185]

David, L. "Legal Action Against China Unlikely in Orbital Debris Collision." *Space News.* Mar. 13, 2013. [84]

Diffie, W. Hellman, M. "New Directions in Cryptography." *IEEE Transactions on Information Theory,* vol. 22, pp. 644-654. 1976. [20]

Dubois, K. "BACN Improves Communication for Deployed Troops." U.S. Air Force publication. Nov. 27, 2018. https://www.af.mil/News/Article-Display/Article/1698903/bacn-improves-communication- for-deployed-troops/. [193]

Eisenhower, D. "Atoms for Peace Speech." Dwight D. Eisenhower Presidential Library, Museum and Boyhood Home, Press Release. Dec. 8, 1953. https://www.eisenhower.archives.gov/research/online_documents/atoms_for_peace.html. [5]

European Space Agency, Space Debris Office. "ESA's Annual Space Environment Report." May, 18, 2018. [98]

Feder, B. "Satellite Company is Trying Life on its Own." *New York Times.* Jul. 23, 2001. [196]

Federal Communications Commission, Letter to Swarm Technologies, Inc. [in response to application for an experimental authorization]. Dec. 12, 2017. https://apps.fcc.gov/

els/GetAtt.html?id=203152&x=. [50,51]

Federal Communications Commission Notice of Proposed Rulemaking and Order on Reconsideration, Nov. 15, 2018. [203]

Federal Communications Commission Report and Order, "Mitigation of Orbital Debris." Jun. 9, 2004. 19 FCC Rcd 11567 (14). [94,95]

Foust, Jeff. "House Science Committee Approves Space Traffic Management Bill." *Space News.* Jun. 27, 2018. [99]

Foust, Jeff. "Senate Introduces Bill to Streamline Commercial Space Regulations." *Space News.* Jul. 27, 2018. [99]

Geib. C. "The U.S. Government Has No Idea What To Do About Small Satellites." *Futurism.* Apr. 11, 2018. [49]

Globalstar. "Our System." https://www.globalstar.com/en-us/corporate/about/our-technology. [132,133]

Griffin, N. "Americans and the Moon Treaty." *Journal of Air Law and Commerce,* vol. 46, art. 6, pp. 750. 1981. [116]

Gwertzman, B. "Nuclear-Powered Soviet Satellite is Expected to Crash This Month." *New York Times.* Jan. 6, 1983. [70]

Gupta, O. "Iridium, A Global Communication Network." Slides to Presentation in AA27, Innovation in Aerospace and Space Exploration, Stanford University. [131,135,166]

Grush, L. "FCC Approves SpaceX's Plans to Fly Internet-beaming Satellites in a Lower Orbit." *The Verge.* Apr. 27, 2019. [200]

Harris, M. "Here are the Odds That One of SpaceX's Internet Satellites Will Hit Some one." *IEEE Spectrum.* Dec. 17, 2018. [101,102]

Harris, M. "The FCC's Big Problem with Small Satellites." *IEEE Spectrum.* Apr. 10, 2018. [52]

Henry, C. "FCC Fines Swarm $900,000 for Unauthorized Smallsat Launch." *Space News.* Dec. 20, 2018. [52,53,54]

Higginbotham, B. "The Space Economy: An Industry Takes Off." U.S. Chamber of Commerce, Above the Fold. Oct. 11, 2018. [1]

History.com Editors. "First Transatlantic Telegraph Cable Completed." *A&E Television Networks.* Last updated: Feb 25, 2019. https://www.history.com/this-day-in-history/first-transatlantic-telegraph- cable-complete. [139]

Inter-Agency Space Debris Coordination Committee. "IADC Space Debris Mitigation Guidelines." Sept. 2007. [91]

International Cable Protection Committee. https://www.iscpc.org/. [147]

Iridium. "Overview Everywhere Under the Sky." https://www.iridium.com/network/globalnetwork/. [130]

Jakhu, R., Jasani, B., McDowell, J. "Critical issues Related to Registration of Space Objects and Transparency of Space Activities." *Acta Astronautica.* vol 145, pp. 406-420. 2018. [108,113]

Joe. L., Porche, I. "Future Army Bandwidth Needs and Capabilities." RAND, Arroyo Center. 2004. [2]

Johnson, Nicholas. "Origin of the Inter-Agency Space Debris Coordination Committee." NASA Technical Reports Server. doc. id: 20150003818, Apr. 1, 2015. [87]

Joux, A. "A One Round Protocol for Tripartite Diffie-Hellman." *Proceedings of the Fourth Algorithmic Number Theory Symposium,* Lecture Notes in Computer Science, vol. 1838, pp. 385-394. 2000. [179]

Kennedy, P. *The Parliament of Man: The Past, Present, and Future of the United Nations.* New York: Random House, 2006. [26,29,30,31,32,33,34]

Kiltz, E., Vahlis, Y. "CCA2 Secure IBE: Standard Model Efficiency through Authenticated Symmetric Encryption." Cryptology ePrint Archive, Report 2008/020. 2008. [186]

Lavallée, B. "The Story Behind the First Reliable Trans-Atlantic Submarine Cable Laid 150 Years Ago." Ciena Publication. Jul. 14, 2016. [140]

Liou, J.C.. "U.S. Space Debris Environment, Operations, and Research Updates." NASA presentation to the Scientific and Technical Subcommittee on the Peaceful Uses of Outer Space, United Nations. Jan. 29 - Feb. 9, 2018. [99]

Lynn, B. "Authenticated Identity-Based Encryption." Cryptology ePrint Archive, Report 2002/072. Jun. 3, 2002. [183]

Madrigal, A. "The Great Pager Blackout of 1998." *The Atlantic.* Mar. 25, 2011. [137]

Manchenton, M. "Airborne Network Gateway Keeps Warfighters on the Same Wave length." MITRE Project Stories. Feb. 2012. https://www.mitre.org/publications/project-stories/airborne-network- gateway-keeps-warfighters-on-the-same-wavelength. [194]

McCormick, P. "The Demise of Intergovernmental Satellite Organisa- tions." *Journal of International Communication.* May 3, 2011. [196]

Mehlitz, P. and Penix, J. "Expecting the Unexpected – Radiation Hardened Software." NASA Ames Research Center publication. https://ti.arc.nasa.gov/m/pub-archive/1075h/1075%20(Mehlitz).pdf. [129]

Menezes, A.J., Okamoto, T., Vanstone, S.A. "Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field." *IEEE Transactions on Information Theory,* vol. 39, pp. 1639-1646. Sept. 1993. [177,178]

Meyer, R. and Starosielski, N. "Managing Risks for the World's Undersea Cable Net work." University of Pennsylvania, Knowledge at Wharton podcast. Nov. 2, 2015. [140,156]

Miller, J. "Repairing a Damaged Submarine Cable: How MainOne Was Put Back in Service." Telegeography Blog. Aug. 8, 2017. [164]

Miller, R. "Another Data Center Planned for Virginia Beach Cable Landing." *Data Center Frontier.* Apr. 28, 2019. [154,155]

Missile Defense Project, "Space Tracking and Surveillance System (STSS)," Missile Threat, Center for Strategic and International Studies, August 11, 2016, last modified: Jun. 15, 2018, https://missilethreat.csis.org/defsys/stss/. [119,120]

Moody, D. et al. "Report on Pairing-Based Cryptography." *Journal of Research of the National Institute of Standards and Technology.* Feb. 3, 2015. [170]

NASA, Astromaterials Research & Exploration Science, Orbital Debris Program Office. "ORSAT." https://orbitaldebris.jsc.nasa.gov/reentry/orsat.html. [102]

National Institute of Standards and Technology, Computer Security Resource Center. "Cryptographic Standards and Guidelines." Last updated: Oct. 10, 2018. https://csrc.nist.gov/projects/cryptographic-standards-and-guidelines/archived-crypto-projects/aes-development. [12]

National Institute of Technology and Standards. Notice, 66 FR 63369. Dec. 6, 2001. [12]

National Oceanic and Atmospheric Administration, NESDIS News and Articles. "Where is Space?" Feb. 22, 2016. https://www.nesdis.noaa.gov/content/where-space. [40]

Neuman, C., Ts'o, T. "Kerberos: An Authentication Service for Computer Networks." *IEEE Communications Magazine.* pp. 33-38. Sept. 1994. [182]

Paar, C, Pelzl, J. *Understanding Cryptography.* Berlin Heidelberg: Springer, 2010. [Fig.1]

Phillips, V. (editor) "Assessing Object Population in Earth Orbit." NASA publication. Last update: Aug. 7, 2017. https://www.nasa.gov/feature/assessing-object-population-in-earth-orbit. [97]

Protection of Submarine Cables, Library of Congress, 24 Stat. 989, Treaty Series 380, Mar. 14, 1884. [141,142,143]

Psiaki, M., Humphreys, T. “Protecting GPS From Spoofers Is Critical to the Future of Navigation.” *IEEE Spectrum.* Jul. 29, 2016. [123,124]

Protocol Concerning the Entry Into Force of the Agreement Between the United Nations and the International Civil Aviation Organization, annex A, May 13, 1947, 8 U.N.T.S. 315. [40]

Qiu, W. “Submarine Cables Cut after Taiwan Earthquake in Dec 2006.” *Submarine Cable Networks.* Mar. 19, 2011. [156]

Rivest, R. Shamir, A. Adleman, L. “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems.” *Communications of the ACM,* vol. 21, pp. 120-126. 1978. [19]

Sechrist, M. “Cyberspace in Deep Water: Protecting Undersea Communication Cables By Creating an International Public-Private Partnership.” Report Prepared for Rand Beers, Under Secretary for National Programs and Protection Directorate, Department of Homeland Security. Mar. 23, 2010. [161]

de Selding, P. “Iridium to Update Hawaii Gateway for Pentagon.” *Space News.* Oct. 31, 2012. [136]

Shamir, A. “Identity-based cryptosystems and signature schemes”, *Advances in Cryptology – Crypto ’84,* Lecture Notes in Computer Science, Vol. 196, Springer-Verlag, pp. 47–53, 1984. [169]

Shan-Hun, C. “Communications chaos in Asia after quake hits Taiwan-Asia-Pacific-International Herald Tribune.” *New York Times.* Dec. 27, 2006. [156]

Sheetz, M. “Morgan Stanley Joins Venture Firms Betting Space Start-up Vector Can Launch A Lot of Small Rockets.” *CNBC.* Oct. 19, 2018. [128]

Sierra Nevada publication. “Revolutionary New Hurricane Satellite System Supported by Sierra Nevada Corporation.” Dec. 15, 2016. https://www.sncorp.com/press-releases/snc-cygnss/. [168]

South-East Asia Japan Cable (SJC) System Overview. *Submarine Cable Networks.* Aug. 12, 2011. https://www.submarinenetworks.com/systems/intra-asia/sjc/sjc-cable-system. [157]

Space Policy Directive-3, National Space Traffic Management Policy. Presidential Memorandum. Jun. 18, 2018. [47]

SpaceX. “Reusability.” https://www.spacex.com/reusability-key-making-human-life-multi-planetary. [128]

Sunak, R. "Undersea Cables: Indispensable, Insecure." *Policy Exchange.* Dec. 1, 2017. [140,144]

Tate, K. "Russian Satellite Crash with Chinese ASAT Debris Explained." *Space.com.* Mar. 8, 2013. [83]

TeleGeography. Submarine Cable Frequently Asked Questions. https://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions. [152,153]

Treaty of Versailles, part 1, Covenant of the League of Nations, preamble, Jun. 28, 1919. [27, 31]

Truman, H. Address in New York City at the Opening Session of the United Nations General Assembly. Harry S. Truman Presidential Library and Museum, Public Papers. Oct. 23, 1946. https://www.trumanlibrary.org/publicpapers/index.php?pid=914. [7]

Tullis, P. "The World Economy Runs on GPS. It Needs a Backup Plan." *Bloomberg.* Jul. 25, 2018. [122]

United Kingdom. Space Industry Act 2018, c. 2, para. 2(h). [55]

United Nations Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space, Apr. 22, 1968, 672 U.N.T.S. 119. [73,74]

United Nations Agreement Governing the Activities of States on the Moon and Other Celestial Bodies, Dec. 5, 1979, 1363 U.N.T.S. 3. [116]

United Nations Committee on the Peaceful Uses of Outer Space, Compendium of Space Debris Mitigation Standards Adopted by States and International Organizations, Feb. 25, 2019. [96]

United Nations Committee on the Peaceful Uses of Outer Space, Report of the Scientific and Technical Subcommittee on the Work of its Thirty-First Session, Mar. 10, 1994, A/AC.105/571. [89]

United Nations Committee on the Peaceful Uses of Outer Space, Legal Subcommittee, The Question of the Definition and/or Delimitation of Outer Space, May 7, 1970, A/AC.105/C.2/7. [40]

United Nations Committee on the Peaceful Uses of Outer Space, Legal Subcommittee, Definition and Delimitation of Outer Space: Views of States Members and Permanent Observers of the Committee, Jan. 18, 2017, A/AC.105/1112/Add.2. [40]

United Nations Committee on the Peaceful Uses of Outer Space, Legal Subcommittee, Status of International Agreements Relating to Activities in Outer Space as at January 2019, Apr. 1, 2019, A/AC.105/C.2/2019/CRP.3. [8,42,64,115,116]

United Nations Convention to Combat Desertification in those Countries Experiencing Serious Drought and/or Desertification, Particularly in Africa, Oct. 14, 1994, 1954 U.N.T.S. 3. [33]

United Nations Convention on International Liability for Damage Caused by Space Objects, Mar, 29. 1972, 961 U.N.T.S. 187. [64,65,66,69,72,78,79,82]

United Nations Convention on the Law of the Sea, Dec. 10, 1982, 1833 U.N.T.S. 397. [33,145,146]

United Nations Convention on the Registration of Objects Launched into Outer Space, Sept. 15, 1976, 1023 U.N.T.S. 15. [106,107,109,112,113,204]

United Nations General Assembly report, Space Debris Mitigation Guidelines of the Committee on the Peaceful Uses of Outer Space, annex 4, Mar. 6, 2007, A/AC.105/890. [90,92,93]

United Nations General Assembly resolution 1472 (XIV), Dec. 12, 1959. [36]

United Nations General Assembly resolution 1721 B (XVI), Dec. 20, 1961. [103]

United Nations General Assembly resolution 1962 (XVIII), Declaration of Legal Principles Governing the Activities of States in the Exploration and Use of Outer Space, Dec. 13, 1963. [38,39,44]

United Nations General Assembly resolution 217 A, Universal Declaration of Human Rights, Dec. 10, 1948. [35]

United Nations General Assembly resolution 2222 (XXI), Treaty on the Principles Governing the Activities of States in the Exploration and use of Outer Space, including the Moon and Other Celestial Bodies, Dec. 19, 1966. [62]

United Nations General Assembly resolution 2777 (XXVI), Nov. 29, 1971. [63]

United Nations General Assembly resolution 3235 (XXIX), Jan. 14, 1975. [106]

United Nations Montreal Protocol on Substances that Deplete the Ozone Layer, Sept. 16, 1996, 1522 U.N.T.S. 3. [33]

United Nations, Note verbale dated 1 June 2017 from the Permanent Mission of the United States of America to the United Nations (Vienna) addressed to the Secretary-General, distr. Dec. 27, 2017, ST/SG/SER.E/803. [112]

United Nations Office of Outer Space Affairs. "United Nations Register of Objects Launched into Outer Space." http://www.unoosa.org/oosa/en/spaceobjectregister/index.html [108]

United Nations, Report of the Second United Nations Conference on the Exploration and Peaceful Uses of Outer Space, Aug. 9-21, 1982, A/CONF.101/10. [59]

United Nations Treaty on the Principles Governing the Activities of States in the Exploration and Use of Outer Peace, including the Moon and Other Celestial Bodies, Jan. 27, 1967, 610 U.N.T.S. 205. [8,42,43,44,45,56,58,61,78,85,86,100,104,199,208]

United States Government Accountability Office, Report to Congressional Requesters. "Intelsat Privatization and the Implementation of the ORBIT Act." Sept. 2004. [196]

U.S. Air Force Fact Sheet. "Defense Satellite Communications System." Nov. 23, 2015. https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104555/defense-satellite-communications-system/. [3,121]

U.S. Air Force Fact Sheet. "Defense Support Program Satellites." Nov. 23, 2015. https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104611/defense-support-program-satellites/. [118]

U.S. Air Force Fact Sheet. "Wideband Global SATCOM Satellite." Mar. 22, 2017. https://www.afspc.af.mil/About- Us/Fact-Sheets/Display/Article/249020/wideband-global-satcom-satellite/. [3]

U.S. Department of Homeland Security and Office of the Director of National Intelligence. "Threats to Undersea Cable Communications." Sept. 28, 2017. [140,150,151,162]

Viega, J., McGrew, D. "The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)." Internet Engineering Task Force, Request for Comments: 4106. Jun. 2005. [24]

Weeden, B. "2009 Iridium-Cosmos Collision Fact Sheet." *Secure World Foundation.* Nov. 10, 2010. [75,76,79]

Wilson, T. "Threats to United States Space Capabilities." Prepared for the Commission to Assess United States National Security Space Management and Organization. *Federation of American Scientists.* Jan. 2001. [2]

Winston, Q. "SEA-ME- WE 5 Consortium Concludes Construction Agreement." *Submarine Cable Networks.* Mar. 10, 2014. [157]

Zeng, C. et al. "All your GPS Are Belong to Us: Towards Stealthy Manipulation of Road Navigation Systems." *Proceedings of the 27th USENIX Security Symposium.* Aug. 15-17, 2018. [125]

Zuckerman, L. "Satellite Failure is Rare, and Therefore Unsettling." *New York Times.* May 21, 1998. [138]

14 CFR §417.19 2011. [110,111]

47 CFR §25.111(b). [192]

51 U.S.C. §50901 (b)(3). 1984. [48]