THE AIR FORCE LAW REVIEW

VOL. 82 **2022**

Authority to publish automatically expires unless otherwise authorized by the approving authority. Distribution: members of The Judge Advocate General's Corps, USAF; judge advocates of the Army, Navy, Marine Corps, and Coast Guard; law schools; and professional bar association libraries.

THE AIR FORCE LAW REVIEW

The Air Force Law Review is a publication of The Judge Advocate General, United States Air Force. It is published semiannually by The Judge Advocate General's School as a professional legal forum for articles of interest to military and civilian lawyers. *The Air Force Law Review* encourages frank discussion of relevant legislative, administrative, and judicial developments.

The Air Force Law Review does not promulgate Department of the Air Force policy. The opinions and conclusions expressed in this publication are solely those of the author and do not necessarily reflect the opinion of The Judge Advocate General, The Judge Advocate General's Corps, or any other department or agency of the U.S. Government.

The Air Force Law Review solicits contributions from its readers. Additionally, readers who desire reprint permission or further information should contact the Editor, *The Air Force Law Review*, The Judge Advocate General's School, 150 Chennault Circle, Maxwell Air Force Base, Alabama, 36112-6418, or e-mail at afloa.afjags@us.af.mil. Official governmental requests for free copies, not under the depository program, should also be sent to the above address.

Cite this law review as 82 A.F. L. Rev. (page number) (2022)

The Air Force Law Review is available online at https://www.afjag.af.mil/Library.

INFORMATION FOR CONTRIBUTORS

The Air Force Law Review publishes articles, notes, comments, and book reviews. The Editorial Board encourages readers to submit manuscripts on any area of law or legal practice that may be of interest to judge advocates and military lawyers. Because *The Air Force Law Review* is a publication of The Judge Advocate General's Corps, USAF, Air Force judge advocates and civilian attorneys are particularly encouraged to contribute. Authors are invited to submit scholarly, timely, and well-written articles for consideration by the Editorial Board. *The Air Force Law Review* does not pay authors any compensation for items selected for publication.

Manuscript Review. Members of the Editorial Board review all manuscripts to determine suitability for publication in light of space and editorial limitations. Manuscripts selected for publication undergo an editorial and technical review, as well as a policy and security clearance as required. The Editor will make necessary revisions or deletions without prior permission of, or coordination with the author. Authors are responsible for the accuracy of all material submitted, including citations and other references. *The Air Force Law Review* generally does not publish material committed for publication in other journals.

Manuscript Form. Manuscripts may be submitted by disc or electronic mail in Microsoft Word format. Please contact the Editor at (334) 953-2802 for submission guidelines or contact the Editor at afloa.afjags@us.af.mil and provide your electronic contact information. Authors should retain backup copies of all submissions. Footnotes must follow the format prescribed by THE BLUEBOOK, A UNIFORM SYSTEM OF CITATION (21st ed. 2020). Include appropriate biographical data concerning the author(s), such as rank, position, duty assignment, educational background, and bar affiliations. The Editorial Board will consider manuscripts of any length, but articles selected for publication are generally less than 60 pages of text. *The Air Force Law Review* does not return unpublished manuscripts.

Distribution. *The Air Force Law Review* is distributed to Air Force judge advocates. In addition, it reaches other military services, law schools, bar associations, international organizations, foreign governments, federal and state agencies, and civilian lawyers.

Cyberspace, Electronic Warfare, and a Better *Jus Ad Bellum* Analogy

*Major Thomas R. Burks**

* Major Thomas R. Burks, USAF, (LL.M., Space, Cyber and Telecommunications Law, University of Nebraska-Lincoln, College of Law (2019); J.D., Indiana University School of Law-Indianapolis, *cum laude* (2010); B.A., History & Philosophy, Indiana University, Purdue University-Indianapolis (2003)) is the Chief of Intelligence Law for 16th Air Force, Joint Base San Antonio-Lackland, Texas. He is a member of the Indiana bar.

I. Introduction

The advent of cyberspace and subsequent development of its many applications has transformed both the public and private sectors like few technological developments before it. Though much of this innovation has proven beneficial, the rapid pace of cyberspace development has often outstripped the law's ability to address those innovations which are not. In particular, reconciling state cyberspace operations with the international law applicable to armed conflict has proven difficult. This body of law is divided into two broad categories: the law governing the conditions under which states may lawfully resort to armed force—the *jus ad bellum*—and the law governing the manner in which belligerents fight once a conflict has commenced—the *jus in bello*.[1] The *jus ad bellum* and its reconciliation to cyberspace operations is the focus of this article.

The modern *jus ad bellum* is rooted in the idea of "force," a concept that will later be covered in greater detail. For now, it is enough to note that Article 2(4) of the United Nations Charter prohibits the use or threat of force unless a narrow exception applies.[2] Consequently, the threshold matter in any *jus ad bellum*-related analysis is whether a particular action amounts to a threat or use of force. The issue is deceptively straightforward, and particularly so in the case of cyberspace operations which do not look or act like what is typically considered a use of force. Malicious code does not, for instance, bear any resemblance to a ballistic missile or an armored column. The critical issue, then, is what exactly does force look like when perpetrated through a cyberspace operation?

Much scholarly ink has been spilled trying to develop an analytical tool capable of a ready response to this question. It should be acknowledged that cyberspace operations approaching the use of force threshold are exceedingly rare. However, the time and attention provided this limited category of state actions is warranted given that states are not limited to an in-kind response to a cyberspace attack. Indeed, a state that finds itself the victim of an armed attack perpetrated through cyberspace could conceivably respond with conventional armed force.[3] An analytical model that distinguishes between force and non-force in cyberspace is thus a matter of considerable importance, as the potential consequences of Article 2(4)-breaching cyberspace operations are as grave as they are rare.

Of the efforts to date, the consequentialist approach of the Tallinn Manual on the International Law Applicable to Cyber Warfare (Tallinn 1.0) and its second edition, Tallinn 2.0, has gained the most traction.[4],[5] Under the Tallinn approach,—referred to hereafter as the "effects model"—a cyberspace operation is a use of force if its effect is *analogous* to the effect of a kinetic or non-kinetic

use of force.[6] The effects model's employment of analogy is unremarkable, as the use of analogical tools is quite common in legal analysis. What is unusual is the extent to which the effects model's analogy departs from the traditional *jus ad bellum* analysis, which has always focused on the modality used (armed force) to determine whether a state action violates Article 2(4). Not so under the effects model's approach to cyberspace operations, which purports to analogize effects but makes no similar claim on the means used to create those effects.

Deviating from a time-honored approach is not necessarily wrong, of course, but it should be done carefully and in full consideration of whether the traditional model has proven insufficient. As the following analysis will demonstrate, the traditional means-focused approach to the *jus ad bellum* was abandoned prematurely in favor of an imprecise effects-based model that is workable in only a small category of cases, and worse yet, threatens to undermine the *jus ad bellum* framework of the UN Charter. Exacerbating this flaw is the fact that operations approaching the scale of this small category have not occurred and are unlikely to, which results in applying the effects model to scenarios to which it is least analytically suited. The result is that in the world of cyberspace operations as they actually exist, the effects model falls short of the mark.

Avoiding these pitfalls and successfully reconciling cyberspace operations to the *jus ad bellum* lies not in wholly abandoning a means-based test or in embracing a purely consequential comparison, but rather in analogizing cyberspace operations to a type of armed force it closely resembles, namely, electronic warfare. Electronic warfare and cyberspace operations are remarkably similar in how they work, how they are used, and even in their limitations. By virtue of these shared characteristics, electronic warfare is able to analogically bridge the gap between armed force and cyberspace operations, thus permitting analysis under a more traditional *jus ad bellum*. The result is a more precise analogy capable of analyzing the world of cyberspace operations as it exists, and of doing so in a manner that upholds, rather than undermines, the UN Charter framework.

In making the case for this new analogical model, this article will begin in Part II with a brief history of the *jus ad bellum* and efforts to date to apply its legal principles to cyberspace operations. Part III begins with the characteristics of strong legal analogies and then demonstrates the level of similarity between cyberspace operations and electronic warfare. Part IV analyzes the wisdom of adopting the proposed analogical model in light of the text and purpose of the UN Charter, as well as how the UN Charter has been interpreted by the International Court of Justice and by state practice in the cyberspace context. Part V provides three principles to guide application of the electronic warfare-cyberspace operations analogy,

and Part VI completes the analysis by demonstrating the fundamental weaknesses of the effects model. Finally, in Part VII, the article concludes with final thoughts on the wisdom of using the electronic warfare-cyberspace operations analogy. The ultimate conclusion is that the effects model was a step too far and it is time for a return to judging cyberspace operations through a more traditional approach to the *jus ad bellum*.

II. *Jus Ad Bellum* – A Brief History

The modern *jus ad bellum* has its origins in the 1648 Peace of Westphalia, a series of treaties that ended Europe's Thirty Years War and established principles designed to prevent war in the future.[7] This contribution to peaceful dispute resolution was short-lived, however, and by the nineteenth and early twentieth centuries states considered themselves free to "wage war … without reservation … for any reason on earth."[8] To the extent the *jus ad bellum* even existed during this period, whether its requirements were met was entirely the business of the state that wished to wage it.[9]

Coinciding with this mindset was an explosion of technological development and industrial capacity that produced new and more powerful weapons.[10] Consequently, an era in which states were somewhat cavalier about resorting to war happened to correspond with the ability to kill large numbers of people with ever greater efficiency. Perhaps as a result of this industrialization of warfare, the idea that a state may resort to war wherever and whenever it wants began to erode. The Hague Convention (II) of 1907, for instance, expressly forbade using war as a means of collecting contract debts.[11] This rather modest restriction did little to prevent World War I, but it was nevertheless a start. Following World War I came the League of Nations, which declared all wars a "matter of concern" for its member states and permitted collective action should the "peace of nations" be threatened.[12] Notably, the League of Nations did not prohibit war as such; it simply made war the rest of the world's business. Facial remediation of this issue came via the Kellogg-Briand Pact of 1928, in which member states renounced war as an "instrument of national policy."[13] By the late 1920s, then, the *jus ad bellum* consisted of an outright prohibition on war for at least the Kellogg-Briand Pact's members states if not also as a matter of customary international law. However, the Kellogg-Briand Pact's failure to define "war"[14] and the ability of states to adopt very expansive concepts of self-defense made this prohibition anything but ironclad, as the widespread death and destruction of World War II readily demonstrated.[15]

In the final months of World War II, the leaders of 50 nations came together in an effort to remediate the failures of the past. The end result of their collaboration was the United Nations,[16] a group and international agreement (the UN Charter) that would eventually include 193 member states.[17] Of the many important provisions in the UN Charter, perhaps the most profound is Article 2(4)'s requirement that member states "refrain in their international relations from the *threat or use of force* against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."[18] Like many areas of law, however, the UN Charter includes exceptions to its general rule. The first is Article 51's recognition that a state has an inherent right to self-defense when it has been the victim of an "armed attack."[19] Second, the threat or use of force is permitted when it is authorized by the UN Security Council.[20]

The modern *jus ad bellum*—the law governing the conditions under which states may lawfully resort to force—therefore consists of a general prohibition on the use or threat of force accompanied by two narrow exceptions[21] and, depending on who one asks, a tolerance for uses of force which do not cross a *de minimis* threshold.[22] This distillation of the *jus ad bellum* is easy to articulate but is often very difficult to apply. For instance, what exactly is "force"? As alluded to in the introduction, the majority position is that Article 2(4)'s prohibition on "force" is really a prohibition of *armed* force.[23] In the context of this writing, the question becomes how that standard should be applied to state actions like cyberspace operations that bear little resemblance to armed force. In fact, cyberspace operations often look more like espionage, political coercion, and economic coercion, none of which violate Article 2(4) despite the fact that such things are harmful to the state at which they are directed.[24]

Efforts to reconcile the *jus ad bellum* to cyberspace operations have generally fallen into one of three categories. The first is the instrumentality approach, which looks at how an operation is executed. The critical question here is whether armed force was used.[25] If so, the operation was likely a use of force; if not, it was not. The second approach is a *per se* rule based on classification of the target. The issue here is whether the cyberspace operation penetrated a target in a designated category.[26] If so, the operation was a use of force. The last approach, the effects model, focuses on the consequences of the cyberspace operation to determine whether a violation of Article 2(4) has occurred.[27] Notably, as in the physical world analysis, the effects model excludes cyberspace espionage,[28] economic coercion, and political coercion from the use of force analysis.[29]

Of the three models outlined above, the effects model has gained the most traction among western states.[30] Under the effects model, a cyberspace operation violates Article 2(4) when its effects are comparable to "non-cyber" operations that violate Article 2(4).[31] More specifically, a cyberspace operation is a use of force if its "scale and effects" are "analogous to other kinetic or non-kinetic actions that the international community would describe as uses of force."[32] A key characteristic of this approach is its reliance on analogy, and more particularly, to an analogy of effects alone rather than a comparison of the means used to create the effects. The viability of the effects model as an analytical tool is necessarily tied to the strength of its analogical approach. Indeed, its usefulness rises and falls thereon, which begs the question, is the analogy a good one? More importantly, is it the best one available? The following section begins a deeper look into these questions by first outlining the characteristics of strong legal analogies, and then examining the viability of an alternative model—the electronic warfare-cyberspace operations analogy—through the lens of these overarching principles.

III. Analyzing Analogy – Cyberspace to Electronic Warfare

Analogy is a powerful tool in legal analysis. Properly employed, it ensures similar cases are treated similarly, provides sound legal bases for decisions, and affords insight into how new issues can be resolved in the future.[33] The idea behind analogy is that because two items share some characteristics, they should be treated similarly because of those shared characteristics.[34] In other words, the two should be treated the same because they basically are the same. Focusing on similarity alone, however, does not necessarily result in a useful analytical tool. Instead, the analogy must also "appeal to a sense or intuition … that it would be *wise* to treat the two items similarly …."[35] An analysis of analogy must, therefore, answer two questions: how alike are the items being compared, and, assuming they are similar, is it a good idea to treat the two items the same?

In the context of cyberspace operations, the issue becomes whether some form of state action or some tool in state arsenals so resembles cyberspace operations that it makes sense to consider them the same for Article 2(4) purposes. Under the traditional approach, this means comparing cyberspace operations to a form of conventional armed force. Cyberspace operations unfortunately do their best to defy such comparison; data manipulating other data bears little resemblance, for instance, to the use of a cruise missile.[36] Mimicking methodology (the "armed" part of armed force) seems, at least at first blush, an impossibility.

Nevertheless, before entirely relinquishing traditional notions of force, it is worth considering whether *any* form of conventional armed force closely resembles cyberspace operations. As the analysis below reveals, there is one—electronic warfare—that offers such a comparison. What follows is an overview of the characteristics shared by electronic warfare and cyberspace operations, and an examination of how the two differ in an important respect. As will be revealed, their similarities and how they are different create a potent comparison—one that can be gainfully analogized for Article 2(4) purposes.

A. Shared Characteristics

The electromagnetic spectrum (EMS) is a concept used to describe and organize the range of electromagnetic radiation, which is, in essence, all of the invisible waves of energy passing through the universe.[37] Electronic warfare is "military action involving the use of electromagnetic and directed energy" to attack an adversary or control the EMS in some way that is favorable to the military doing the controlling.[38] Cyberspace operations, on the other hand, involve the use of devices or computer programs to create some effect in "cyberspace,"[39] which the Department of Defense defines as "interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[40]

Based solely on these definitions, electronic warfare and cyberspace operations appear to have little in common. Upon closer examination, however, the similarities are manifold. Beginning with the broadest similarity, cyberspace operations and electronic warfare are both non-kinetic.[41] A kinetic action is one that uses the "motion of material bodies and the forces and energy associated therewith" to cause some effect in an object.[42] A *moving* bullet damaging the human body as its *energy* is expended after impact a good example. The destructive energy produced by an exploding bomb or high explosive artillery shell is another.

Non-kinetic actions are the reverse, meaning they achieve some result without relying on the movement of material bodies and associated energy.[43] An electromagnetic pulse weapon, for example, "kills" a machine by using electromagnetic radiation to overwhelm and destroy its electrical circuitry.[44] Following such a pulse, the targeted machine is almost certainly non-functional, but its structural integrity is likely intact. A cyberspace operation that causes an electrical surge in a machine and destroys its electrical circuitry produces the same result. While the machine no longer functions, the structure of the machine is likely still whole. Neither operation required the energy of a moving object to achieve its effect, which means both are examples of non-kinetic action.

In addition to being non-kinetic, cyberspace operations and electronic warfare share a similar range of capabilities. Both can deny use of the EMS, which implicates things like command and control systems, wireless networks, cellular service, and radar systems.[45] Additionally, both are capable of deception operations,[46] surreptitious intelligence collection,[47] and, under the right conditions, of damaging or destroying physical objects.[48] What's more, both electronic warfare and cyberspace operations can employ these capabilities offensively and defensively.[49] The mission profiles of both run the gamut from intelligence collection to physical destruction, which, in practical effect, means they are capable of executing operations on both sides of Article 2(4)'s prohibition on the threat or use of force.

In addition to being non-kinetic and having comparable operational ranges, electronic warfare and cyberspace operations are also similar in that both rely on the EMS. Electronic warfare's connection is readily apparent; without the ability to manipulate the EMS, electronic warfare would not exist. The EMS-to-cyberspace connection is somewhat less obvious, given that cyberspace operations may be conducted through wired networks. However, the ubiquity of wireless networks and mobile computing devices (which now includes aircraft and other vehicles), all of which rely on the EMS for connectivity, means that the path to targets exploitable through cyberspace is increasingly through the EMS.[50]

Even more fundamentally, however, is the fact that cyberspace is not just comprised of networks, computers, and systems that *use* the EMS, but rather has its roots in the EMS itself.[51] Cyberspace, wired or otherwise, is based on electromagnetic physics. Accordingly, though it has various human made components layered onto it, the EMS is the larger domain in which cyberspace resides.[52] Thus, while it uses various components as a means of navigation, a cyberspace operation is fundamentally "information[] traveling through the spectrum."[53] Consequently, whether viewed holistically as based in the EMS or as simply passing through it en route to a target, cyberspace operations and the EMS are inextricably connected. It should come as no surprise, then, that cyberspace operations and electronic warfare are increasingly thought of as common members of a non-kinetic arsenal that states can use singularly, together,[54] and even interchangeably.[55]

It is here that the closeness of the electronic warfare-cyberspace operations relationship is fully revealed. Their common origin in the EMS moves the comparison beyond generic functional categories and into practical application. In fact, as the following examples demonstrate, it can be difficult to determine which tool was used in a particular operation.

On September 6, 2007, Israeli strike aircraft crossed into Syrian airspace and bombed a nuclear reactor in northern Syria, thereby reducing it to rubble.[56] Interestingly, despite having a fully functioning and very capable air defense system, the Syrian military was unaware of the Israeli presence until bombs began exploding.[57] According to one author, the Israeli infiltration was made possible through the use of electronic warfare used against Syrian air defense systems.[58] Another author, however, suggests that it was a cyberspace operation that made Syrian airspace appear empty on radar screens.[59] Which author is correct is impossible to tell. Given that "a digital stream of computer code or a pulse of electromagnetic power can both be used to create false images in adversary computers," the point is that either, or the two combined, could be the culprit.[60]

Consider also that in 2015, two cybersecurity researchers demonstrated their ability to access a Jeep Grand Cherokee's onboard computer system through a vulnerability in its software.[61] After wirelessly accessing the vehicle, the researchers proceeded to turn on windshield wipers and change radio stations, among other forms of mischief.[62] On the more serious side, the researchers proved it was possible to remotely shut off the vehicle's engine while the driver was traveling down the highway.[63] Contrast this with the United States military's Radio Frequency Vehicle Stopper, which uses high-powered microwave radiation to stall a vehicle's engine by causing its onboard computer to reboot over and over.[64] Importantly, both the electronic warfare method and the cyberspace operation achieved a similar result by targeting the same type of onboard systems.

Finally, cyberspace operations and electronic warfare are alike in that they share common limitations. Both are examples of what Professor Martin Libicki calls "non-obvious warfare," a category of state actions characterized by their ambiguity.[65] In fact, the target of a non-obvious warfare operation may not realize anything has happened, and even if it is aware of a problem, determining whether it resulted from an accident or purposeful action can be difficult.[66] Further, even if purposeful action is a certainty, attributing that action to a particular actor is an additional challenge.[67] This inherent ambiguity means that forms of non-obvious warfare, like cyberspace operations and electronic warfare, are ideally suited for scenarios in which the actor wishes the victim to remain uncertain as to its identity.

This common utility also highlights a common limitation: electronic warfare and cyberspace operations are rather poor strategic weapons. Neither is capable, for instance, of conquering and holding territory, although they certainly enhance the ability of states to pursue those aims.[68] Neither are they capable of specific coercion in that the state being coerced must understand who is doing the coercing in order for it to work.[69] The practical effect of these limitations is that to the

extent a cyberspace operation or use of electronic warfare is apparent, it is likely because it was used to enable a more traditional use of force. The Israeli strike against the Syrian nuclear reactors is an excellent example. However, when used in a standalone capacity or perhaps together, cyberspace operations and electronic warfare are most likely to be used surreptitiously and in very understated ways.

B. The Difference Between

Though they share many characteristics, it is important to note that cyberspace operations and electronic warfare are not precisely alike. While both do similar and sometimes exactly the same things, the manner in which they do them is different. Perhaps the most significant difference is that while cyberspace operations are holistically part of the EMS, they occur in a human made construct comprised of three different layers, any one or more of which can be targeted.[70] The first layer is the physical infrastructure that forms cyberspace's real-world existence; the "tubes" of the Internet[71] and the "wires, routers, and switches" of networks generally.[72] The second is the syntactic layer that "reflects both the format of information in cyberspace and how the various information systems from which cyberspace is built are instructed and controlled."[73] The final layer of cyberspace is semantic, which is "the information meaningful to humans or connected devices."[74]

Compare this to electronic warfare, which has many applications but is comprised of a single "layer" that manipulates the power and energy of a naturally existing physical domain (the EMS) in ways that affect the object at which it is aimed. In other words, physical force aimed at objects that are susceptible to that physical force. It is this characteristic that makes electronic warfare a form of armed force.[75]

Cyberspace operations are thus part of the EMS but use information passing through it to achieve objectives in one or more of three human made layers, whereas electronic warfare uses and manipulate the EMS itself. This distinction looms large, but it is essential to remember that *similarity*, not identicality, is the key to a robust analogical model. If the two were identical, an analogy would be unnecessary because the items compared would in fact be the same thing.[76] Thus, that differences exist between two otherwise remarkably similar items is not necessarily the death of the analogy. This is particularly true when, as is the case here, the differences are what makes the analogy feasible.

C. Reconciling the Difference

Simply put, electronic warfare is just different enough from cyberspace operations for the use of force in the latter to be identifiable by comparison to a use of force in the former. To understand why this is, one must first understand the interplay between international law, the categories into which state actions typically fit, and how the targets of those state actions—data, human thought, and machines—fit into that dynamic. Once this is grasped, the utility of electronic warfare as a comparator comes into full relief and demonstrates its ability to analogically bridge the gap between armed force and cyberspace operations. Importantly, electronic warfare not only enables this comparison, but also helps distinguish cyberspace operations from forms of state action that do not employ armed force and thus, while perhaps gravely damaging, do not implicate Article 2(4).

State actions implicating international law generally fall into one of four categories: economic coercion, political coercion, espionage, and armed force.[77] While it is helpful to have categories into which state action can be placed, the categories themselves provide little guidance as to how a particular action should be classified. Categorical difficulty is not always at issue; there is little danger of mistaking an economic sanction for conventional armed force and vice versa. However, the absence of guidance is a problem with cyberspace operations, which may be capable of actions that fit all four groups. To remedy the categorization issue, it is helpful to consider these four areas in terms of what they aim to do.

Espionage is the obtaining of "information about the plans and activities … of a foreign government"[78] so that it can be used to "design more concrete instruments [of foreign affairs] or policies."[79] The purpose of espionage is thus the procurement of data—ideally without the party from whom it was procured finding out. By contrast, the purpose of economic and political coercion is rather different. Whether in the form of hunger pangs and joblessness following an embargo, or carefully crafted propaganda or disinformation at election time, both forms of coercion seek to influence the way people think and thereby influence their actions. Armed force, quite different from the others, seeks to coerce through the administration of death and destruction or the apparent ability to cause those things. It is by nature violent, though its character—how it is violent—can take many forms.[80]

From these purposes, one can distill three categories of state action: state action that targets information (akin to espionage); state action that targets the human mind (akin to economic/political coercion); and state action that targets the structural integrity of objects and people (akin to armed force). Viewed through a cyberspace lens, these categories can be conceptualized as: sending data to target the human mind; sending data to target other data alone; and sending data to target machines.[81] The first two types of cyberspace operations (data to data and data to the human mind) are not uses of force, but the third category (data to machines) might be. The question, then, is how to separate the forceful cyberspace wheat from the non-forceful chaff?

It is here that electronic warfare lends a helping hand. Consider a directed energy weapon that uses high-powered microwaves (HPM DEW) against its targets. When an HPM DEW is "fired," the pulse finds its way into the target through a port and then uses the target's electronic pathways to overload and overwhelm its circuits, or, once inside, radiates its energy throughout the target where it is picked up by circuit boards and processors.[82] The result is overloaded components that fail because they cannot withstand the power of the pulse,[83] thereby destroying the object's functionality though perhaps not its structural integrity.[84] In essence, the HPM DEW directs the power of electromagnetic radiation—something the object is designed to use—in a way that overwhelms and destroys the object at which it is directed. In doing so, it looks and acts like a weapon, which is perhaps why there seems to be little, if any, doubt as to whether electronic warfare is a form of armed force.

But is a cyberspace operation capable of doing the same? In one sense the question must be answered in the negative; a cyberspace operation cannot do precisely what an HPM DEW does. However, when viewed in a somewhat broader sense it is clear that cyberspace operations have very *similar* capabilities. For instance, a cyberspace operation is capable of harming or even destroying the functionality of a machine.[85] More importantly, a cyberspace operation is capable of sending data to a machine and interacting with it in a way that harnesses the machine's internal power to damage or destroy it. Stated another way, data can hijack the power of a machine and cause it to destroy itself and things around it with the very capabilities it was designed to use. This concept of operations is not *exactly* the way an electronic warfare capability works, but it is exceptionally similar.[86]

It is on this point of similarity that electronic warfare shines brightest as an analogical comparator. Electronic warfare is accepted as a form of armed force even though it looks and acts more like a cyberspace operation than kinetic or even other non-kinetic forms of armed force.[87] It is this dual status—armed

force that looks and acts like cyber—that allows electronic warfare to create an analytical bridge between conventional uses of force and cyberspace operations. The result is an analogical model that accounts for both the effect and the method of a cyberspace operation and thus permits analysis under the traditional, armed force-focused approach to Article 2(4).

A note of caution is warranted here. Under the proposed analogical model, the fact that a cyberspace operation hijacked the power of a machine is not sufficient to render it a use of force. Instead, to constitute a violation of Article 2(4), it must harness the power of the object in a way that mimics or very closely resembles an electronic warfare capability. Electronic warfare's ability to use and manipulate the power of a physical domain is the very characteristic that qualifies it as a form of armed force.[88] Thus, any cyberspace operation successfully analogized to it "must closely resemble not only the effects but also the acts" it is capable of performing.[89] Fortunately, the two are otherwise so similar that the distinction enables the analogy and makes it viable. The issue remains, however, whether the electronic warfare-cyberspace operations analogy is also sensible. It is to this issue that the next section turns.

IV. The Wisdom of Common Analysis

The sheer similarity of electronic warfare and cyberspace operations suggests that an analogical model comparing the two is worthy of adoption. However, similarity alone is not enough; an analogical model must also "appeal to a sense or intuition … that it would be *wise* to treat the two items similarly …."[90] As will be demonstrated, an analogical model comparing cyberspace operations to electronic warfare is prudent for three reasons. First, it is faithful to the text of the UN Charter and thus to the modern *jus ad bellum*. Second, the proposed model is consistent with the purpose of the UN Charter and to how Article 2(4) has been interpreted since entering force. Finally, the proposed analogy is in harmony with trends in state practice in the cyberspace operations context. These factors, combined with shared characteristics, indicate that treating cyberspace operations and electronic warfare alike for the use of force analysis is indeed a sensible choice.

A. Textual Consistency

The UN Charter's text and formative context, as well as its preparatory materials, suggest that Article 2(4)'s prohibition on force is actually a prohibition on *armed force*.[91] Beginning with the text, it must be acknowledged that the word "armed" is glaringly absent from Article 2(4).[92] However, in the preamble, the UN Charter provides that its member states executed the agreement to save future generations

from the "scourge of war," which had twice in the span of a generation "brought untold sorrow to mankind."[93] To prevent future scourges, members pledged to "unite in strength to maintain international peace and security" and ensure that "*armed force*" is not used except in the common interest.[94] The UN Charter goes on in Article 1 to list the purposes for the treaty's existence, which notably include maintaining international peace and security as the first item.[95] In order to achieve these aims, members of the United Nations are required to settle international disputes in ways that do not disrupt international peace and security[96]—a provision which is immediately followed by Article 2(4)'s prohibition on the use or threatened use of force.[97]

These passages from the UN Charter can be collectively restated as follows: war is the "scourge" of humankind, and to avoid it in the future, member states must forego the use of armed force as a means of international dispute resolution; accordingly, the use or threatened use of force—meaning armed force—is prohibited. This summation is substantiated by Article 44 of the UN Charter, which uses "force" unmodified by "armed," but does so in a way that clearly contemplates armed force.[98] When the text of the UN Charter is read holistically in this manner, it is apparent that Article 2(4)'s prohibition is squarely aimed at preventing acts of armed force that can lead to the "scourge" of war.[99]

This textual interpretation is corroborated by subsequent state action in the form of United Nations General Assembly Resolution 3314,[100] which defined acts of aggression as the "use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with" the purpose of the UN Charter.[101] Importantly, the language used to define "act of aggression" is nearly identical to that of Article 2(4), which indicates an act of aggression and use of force are the same in concept if perhaps different in degree. The key takeaway from Resolution 3314 is that when the nations of the world had an opportunity to comment on what Article 2(4) means, the term "armed force" was used and every example provided (invasion, bombardment, blockades, etc.) was a form of conventional armed force.

However, because "armed" is missing from Article 2(4), there is room for an alternative interpretation, which suggests the text of Article 2(4) is ambiguous. To satisfactorily resolve this ambiguity or to at least reinforce the above interpretation, it is helpful to consider the circumstances surrounding the treaty's conclusion and the record of its drafting.[102] While the UN Charter did not enter force until a few months after World War II ended, it was signed by the original member states on June 26, 1945 while the war was very much ongoing.[103] Recall also the string of unsuccessful international agreements that failed to prevent World War II

in the first place. To close the loopholes left in previous international agreements, the UN Charter sought to prohibit "force" instead of "war."[104] In other words, in order to prevent another war the UN Charter prohibited those acts of which war is comprised, namely, uses of armed force.[105]

The preparatory work of the UN Charter further supports reading the word "armed" into Article 2(4). A majority of the committee that finalized the language of Article 2(4) considered and even favored incorporating economic coercion into the prohibition on the threat or use of force.[106] However, the greater United Nations conference ultimately declined to do so, and while this does not clearly limit Article 2(4) to armed force, it does exclude economic coercion and things akin to it from Article 2(4)'s prohibition.[107] Coupled with the position that political coercion and espionage are also not uses of force, the exclusion of economic coercion from Article 2(4) strongly suggests, by process of elimination, that the prohibition against the threat or use of force is really a prohibition on *armed* force.

With this textual interpretation in hand, the question becomes what significance it holds for the electronic warfare-cyberspace operations analogy? The answer is twofold. First, analogizing a cyberspace operation to a substantially similar form of armed force enables analysis consistent with a textual interpretation of the UN Charter and thus under the traditional means-based approach to the *jus ad bellum*. Stated another way, the electronic warfare-cyberspace operations analogy permits analysis under the law as it has existed since at least 1945. Second, by prohibiting the threat or use of armed force rather than all forms of state coercion, Article 2(4) makes the instrument of state action legally determinative, meaning one particular form of state coercion can violate Article 2(4), while others cannot even if damaging and perhaps even unlawful under other provisions of international law. Consequently, a comparison that analogizes the means used in state action, and not just its effects, helps distinguish actions that might violate Article 2(4) from those that never will.

The contrast between armed force and economic and political coercion helps illustrate this point. Economic sanctions are a form of economic coercion through which states seek to change the behavior of another state by targeting its economy. However, while economic downturn may be the primary result, the impact of economic sanctions can be far graver and even fatal, as Iraq's experience in the 1990s indicates.[108] Yet, despite the potential for very severe consequences, economic coercion is not a use or threat of force. Consider also the potentially harmful effects of election meddling, which is a form of political coercion. Nations of the world have long interfered with the elections of other governments. A declassified report from the Central Intelligence Agency (CIA), for instance, outlines efforts by the

CIA to influence the outcome of Chile's elections in 1964.[109] Even more notorious is Russia's cyberspace-focused meddling in the 2016 presidential election in the United States. Both operations arguably threatened the political independence of the target nations. Nevertheless, the rhetoric of some officials notwithstanding,[110] neither instance of political coercion is considered a threat or use of force.[111]

The foregoing examples beg the question of why, given the negative (even fatal) effects of political and economic coercion, neither is a violation of Article 2(4). The answer is that neither employs armed force to achieve its ends. Simply stated, no matter how terrible the result, the lack of armed force places political and economic coercion in a different category of legal analysis.[112] It is clear, then, that the method of state coercion matters a great deal in the use of force analysis. Consequently, an analogical model seeking to reconcile cyberspace operations to Article 2(4) in a way that is consistent with a textual interpretation of the UN Charter and avoids conflating such operations with non-force forms of state action, must necessarily be able to link the operations to a form of armed force. This demonstrates the value of an analytical model like the electronic warfare-cyberspace analogy that does this very thing.

B. Consistency of Purpose

In addition to being textually consistent, the electronic warfare-cyberspace operations analogy is also consistent with the primary purpose of the UN Charter: to maintain international peace and security.[113] As previously mentioned, the immediate context that gave birth to the UN Charter indicates that to its drafters maintaining international peace and security meant avoiding things like "Hitler's tanks driving over the Polish border or Japanese planes bombing Pearl Harbor."[114] Consequently, rather than repeating the broad prohibitions of already failed international agreements, the UN Charter instead prohibits "force." Given that "force" is the modern-day equivalent of the term "act of war,"[115] it seems the UN Charter seeks to avoid war by prohibiting, not just war in the worldwide hostilities sense, but also actions falling far short of it. By preventing the lesser actions, the UN Charter, in theory, prevents a more significant breach to international peace and security. From this perspective, an expansive concept of force makes sense. Including more types of coercive action in Article 2(4)'s prohibition keeps a tighter rein on member states, thereby ensuring no one comes close to upsetting international peace and security by resorting to the "scourge" of war.[116]

Notably, however, the UN Charter did not establish a one world government superior in authority to the states comprising it. Indeed, in Article 2 it expressly recognizes the "sovereign equality" of each member state,[117] which means each state very much remains its own boss. Implicit in this preservation of sovereignty is the right of states to pursue their interests, even if those interests conflict with those of other states. These self-interested pursuits inevitably breed friction, and although the UN Charter requires states to use "peaceful means" of dispute resolution,[118] "peaceful" does not mean coercion-free.[119] Consequently, though the UN Charter seeks international peace and security, it leaves intact the state sovereignty-based international order that led to many wars in the past. This remainder is a recipe for inter-state conflict even if it is ultimately settled peacefully.

In addition to individual sovereignty, the UN Charter also preserves a state's inherent right to defend itself when it is the victim of an armed attack.[120] The result of this sovereignty/self-defense conglomeration is that while the UN Charter was formed to maintain international peace and security, it remains hard-wired with the components necessary to spark an armed conflict. All this tinderbox requires is a use or threat of "force" of sufficient gravity. When viewed from this perspective, a broad concept of force makes little sense; Article 2(4) should capture less in order to prevent states from going to war by invoking the right of self-defense too easily.

To resolve the UN Charter's inherent tensions, Article 2(4)'s prohibition must be placed at a middle ground, or "sweet spot," that bars the small actions most likely to lead to wider conflicts, while also not prohibiting so much that a war paradoxically results. Armed force is the natural place for this "sweet spot." It provides the maneuver space states need to conduct foreign relations below the Article 2(4) threshold, while also providing a more definite point of departure for permissibly invoking Article 51's right of self-defense. The unique characteristics and capabilities of cyberspace operations make adherence to the armed force threshold less clear-cut, but in light of the overall purpose of the UN Charter, adherence is no less an imperative today than it was at the time the balance was originally struck. A comparison to electronic warfare meets this imperative by bridging the gap between cyberspace operations and conventional armed force, thereby maintaining the original Article 2(4) threshold. The electronic warfare-cyberspace operations analogy thus meets the objectives of the UN Charter in the manner in which the UN Charter contemplates, further demonstrating the wisdom of adopting it as an analytical tool.

C. Interpretive Consistency

Examining the text and purpose of an international agreement is necessarily the starting point of interpretive analysis. However, treaties are not created and implemented in a vacuum. Just as the parties to a commercial contract can differ on the meaning of their obligation, states too can differ in their interpretation of the legal obligations in an international agreement or a rule of customary international law. This is why state practice is essential to treaty interpretation, and by extension, why decisions by tribunals applying the law to those state actions can be helpful as a "subsidiary means" of interpretation.[121] One such judicial decision, *Nicaragua v. United States*, is the focus of this section. As the following indicates, the *Nicaragua* decision expanded the concept of force, but it did so only slightly and in a manner that suggests the prohibition on the use of force is still a prohibition on armed force. Once again, this demonstrates the utility of an analytical model, like the electronic warfare-cyberspace operations analogy, that compares cyberspace operations to a form of armed force.

In the early 1980s, the CIA began a covert operations campaign against the Nicaraguan government that included providing support to the *contras*, a catch-all term describing anti-government Nicaraguan guerillas.[122] To remediate what it perceived to be a violation of its sovereignty, Nicaragua filed a claim with the International Court of Justice (ICJ) and ultimately prevailed in a case that produced a judgement of enduring importance.[123] The *Nicaragua* court made several findings, but the one most germane to the subject of this article is its conclusion that "arming and training" the *contras* amounted to a threat or use of force by the United States.[124] In making this judgment, the court introduced an agency concept into the use of force calculus, and in doing so, arguably broadened the scope of Article 2(4)'s prohibition. When determining the significance of this widening, it is important to note how it was widened and the degree to which the concept of force was actually expanded. Careful scrutiny reveals that Article 2(4)'s prohibition widened only a little, and its expansion did not cut its tether to armed force.

First, the ICJ's determination that arming and training the *contras* was a threat or use of force cannot be divorced from what the *contras* did with that assistance. In its complaint, the Nicaraguan government argued that the atrocities of the *contras* should be attributed to the United States because the arms and training it provided the *contras* in El Salvador was used to wreak havoc in neighboring Nicaragua.[125] The fact that widespread death and destruction was the result suggests that what the *contras* did with the training and arms was just as crucial to the use of force analysis as the actions taken by the United States. This conclusion is particularly fitting in light of the ICJ's observation in the same opinion that "in international

law there are no rules … whereby the level of armaments of a sovereign State can be limited."[126] In other words, El Salvador can arm to the level it wants, train to the level it wants, and even permit an ally like the United States to bring in arms and conduct training activities in its territory. Thus, had the *contras* never crossed the border and taken action, Nicaragua's complaints would likely have been dismissed as attempts to limit what El Salvador, as a sovereign nation, may permit within its borders.

Second, the ICJ rests its use of force conclusion, in part, on UN General Assembly Resolution 2625, which places on states the duty to "refrain from organizing … irregular forces or armed bands … for incursion into the territory of another state … and [to refrain from] participating in acts of civil strife."[127] In applying Resolution 2625, the ICJ observed that organizing irregular forces to engage in civil strife is a use of force if the actions taken by the irregular forces are, in fact, a use of force.[128] Notably absent from the ICJ's analysis is a suggestion that arming and training the *contras* would have amounted to a use of force even had the *contras* done nothing with it. Again, had the *contras* stayed in El Salvador or returned home and lived peacefully, the *Nicaragua* case no doubt would never have been filed.

In the context of this article, the question becomes what significance the ICJ's decision holds for the electronic warfare-cyberspace operations analogy? The key takeaway from this portion of the *Nicaragua* opinion is that while the use of force may be broadened slightly beyond the text of Article 2(4) to include an agency concept, this widening is more of a carefully guarded crack than a throwing open of the door.[129] Indeed, rather than opening Article 2(4) to entirely new concepts of force as some suggest it does,[130] the *Nicaragua* opinion strongly suggests it remains wed to armed force. In fact, the decision did not move the armed force sweet spot at all; it merely plugged a loophole through which states might try to use armed force without technically violating Article 2(4). Additionally, by using Resolution 2625 to support their conclusion, the ICJ applied a principle to which states had already expressed agreement. UN General Assembly Resolutions are not legally binding, but they can provide interpretive guidance on the legal terms to which they apply.[131] Arguably, then, the ICJ broadened the scope of "force" in the Article 2(4) sense exactly as far as state practice had already broadened it. The same cannot be said of cyberspace operations, given the lack of consensus in the international community on what is and is not permissible in that realm.[132]

The bottom line is that the *Nicaragua* decision did not open Article 2(4) to previously uncontemplated forms of force. Instead, the decision indicates that the method used (armed force) still matters even in a slightly expanded use of force analysis. Accordingly, analogically reconciling cyberspace operations to Article 2(4) must be based in something that (1) can be considered a use of armed force, and (2) creates a means of analyzing cyberspace operations that is at most a *slight* expansion of Article 2(4).[133] Again, this points to the wisdom of the electronic warfare-cyberspace operations analogy, which can use electronic warfare's similarity to cyberspace operations to bridge the cyberspace-armed force divide.

D. Consistency with State Practice

Up to this point, Part IV has consisted of examining Article 2(4) as it relates to conventional armed force and then applying those principles to the cyberspace operations context. This analysis is useful and necessary, but to fully demonstrate the utility of the electronic warfare-cyberspace operations analogy, it is essential to examine state action within the context of real-world cyberspace operations. As the analysis below demonstrates, trends in state practice suggest that the method of operation, not just its effect, still very much matters. Once again, this indicates the prudence of an analogical approach like the electronic warfare-cyberspace operations analogy that judges *jus ad bellum*-compliance by comparing cyberspace operations to a form of armed force.

An examination of state action must begin by outlining its significance to the *jus ad bellum*. Simply put, state practice is the single most important component of international law. It forms the basis for customary international law, makes international agreements possible, and gives meaning to these two sources of law by providing real-life interpretation.[134] Judicial opinions and legal commentary are helpful, of course. However, while judicial opinions provide valuable interpretive guidance and some have proved enduring, the opinions of the ICJ bind only the parties to the particular litigation.[135] Commentary from legal experts can also be helpful, but it too is non-binding. It is the ability of states to act, whether by consenting to be bound or through actions interpreting legal obligations previously consented to, that forms the backbone of international law. This concept is as true with the *jus ad bellum* as it is to other forms of international law. Indeed, as Professor Rosa Brooks observed, "war is whatever powerful states say it is."[136] In the same way powerful states define "war," so to do they define what is and is not considered a use of force.

Given the obvious importance of state practice in reconciling cyberspace operations and the *jus ad bellum*, it is noteworthy that to date no standalone cyberspace operation has resulted in a state accusing another of violating Article 2(4).[137] The following analysis attempts to explain why this is by reviewing state responses to two real world cyber events and drawing conclusions therefrom as to how states appear to view the *jus ad bellum* in the cyberspace context. The first case study is an overview of the 2007 distributed denial of service (DDoS) attack in Estonia.[138] The second is an overview of Stuxnet, the clearest and most well-known instance of a cyberspace operation approaching the use of force threshold. As will be demonstrated, state action following these incidents suggests that the *jus ad bellum* remains wed, even in cyberspace operations, to the traditional armed-force focused approach.

On April 27, 2007, information systems in the nation of Estonia became the target of a DDoS attack. A DDoS attack can take many forms, but the basic idea is to create a volume of network traffic so great that the targeted system becomes saturated and can no longer function.[139] The DDoS attack in Estonia was carried out in part via the relatively simple "ping" method, which relies on individual computer users to create the necessary network traffic.[140] It was also carried out through the use of botnets, which are networks of previously hacked computers used in concert to send high levels of traffic to the targeted systems.[141] All told, the Estonian DDoS attack affected web servers, email-servers, and Domain Name System servers and routers, and impacted the office of the Estonian president, its parliament and the police, as well as Internet Service Providers, online media, and the Estonian banking system and other private industry.[142]

Responsibility for the attack has never been definitively attributed, but an examination of motive and opportunity to act is helpful on this point. In the days leading up to the attack, the Estonian government moved a large statue of a Soviet soldier from the center of Tallinn, its capital city, to a military cemetery on the city's outskirts.[143] The move was controversial in Russia and amongst ethnic Russians living in Estonia, who viewed the statue as a symbol of Soviet heroism during World War II and its removal as a slap in the face.[144] Giving voice to their opposition, Russian-speaking Estonians held protests at the statue's site prior to its removal and Russians in Moscow also protested outside of the Estonian embassy.[145] Notably, the DDoS attack began the morning after removal, and was fueled in part by anti-Estonia messaging on Russian websites accompanied by instructions on how to carry out the operation.[146] The attack was also presaged by a statement from the Russian government that removing the statue would be "disastrous for Estonians," and was followed by a remark from Vladimir Putin that

"[t]hose who are trying today to... desecrate memorials to war heroes are insulting their own people, sowing discord and new distrust between states and people."[147]

While these many factors are inconclusive and the Russian government has denied involvement, to the extent the DDoS attack on Estonia can be credited to a particular party it is generally thought to have been the work of or encouraged by the Russian government.[148] It is unsurprising, then, that Estonia sought help from the North Atlantic Treaty Organization (NATO), a body and international agreement which it had recently joined. Article 5 of the NATO agreement states that an "armed attack" against one member state is an attack on the lot of them, and any attack will be responded to collectively with "such action as it deems necessary" to restore the peace and security of the North Atlantic area.[149] NATO notably responded with cybersecurity assistance but it declined to go down the path of Article 5, prompting an Estonian official to comment that "At present, NATO does not define cyber-attacks as a clear military action. This means that … collective self-defence, will not automatically be extended to the attacked country."[150]

Estonian response to the attack, other than cybersecurity measures to stop and protect against it, was ultimately limited to prosecution of a 20-year old student living in Estonia whose participation from inside the country permitted collection of evidence.[151] It is telling that despite the havoc wrought, the resulting economic loss, and the clear political overtones of the action, NATO was unwilling to even consider the cyber-attack as a military action, much less a use of force. NATO states seem to have retreated from the cyber-is-not-military-action position in the years following.[152] However, there is no indication in state practice that a repeat attack would be considered a violation of Article 2(4). In fact, the opposite is true. In December 2011, Iranian nationals believed to have been working on behalf of their government initiated a 176-day DDoS attack against the American banking sector, an incident that ultimately cost tens of millions of dollars to remediate.[153] The United States' response was notably not saber-rattling or Article 2(4)-tinged rhetoric, but rather the indictment of seven of the Iranians involved.[154] In other words, it was treated as a cyberspace-based crime.

State practice following the cyber-attack on Estonia makes perfect sense when viewed through the lens of the electronic warfare-cyberspace operations analogy. What Estonia experienced as a DDoS attack is the electronic warfare equivalent of electromagnetic interference or jamming,[155] which states have used for many years below the use of force threshold.[156], [157] Even more important to the calculus is what the Estonian attack reveals about the target of the operation. It was not a case of data sent to machines to harness the power and function of a machine in a manner similar to armed force. Rather, it has the appearance of political coercion,

meaning data targeting human minds to make a political point.[158] Accordingly, the DDoS attack on Estonia would not have been a use of force under the electronic warfare-cyberspace operations analogy.

The years since the Estonian DDoS attack have seen many malicious cyberspace operations, and while the cyber "Pearl Harbors" warned of in headlines have not materialized,[159] there are operations that have had the potential to cross the use of force threshold. Stuxnet is the clearest and most well-known instance, and yet, though it caused physical damage, the state affected (Iran) never called it a use of force. Nor, for that matter, has any other state. In-depth examination is necessary to understand why that might be and what it means for the interaction of cyberspace operations and Article 2(4). What follows is an overview of Stuxnet and Iran's response to it, followed by conclusions on the state of the law suggested by its example.

Stuxnet was a multi-year cyberspace operation that used software to manipulate the industrial control systems at Iran's Natanz nuclear enrichment facility.[160] It did this to cause damage to centrifuges, which are equipment used to process uranium into fuel for nuclear reactors, and if processed long enough, for use in nuclear weapons. Stuxnet was designed to target the type of system used to control the centrifuges during the enrichment process. Once it found the right target, the software delivered a payload that allowed it to influence the speed with which various components of the machinery moved.[161]

Before actually manipulating those components, Stuxnet recorded readings for normal operations and began sending this data to the system's internal monitors and to the human operators monitoring the enrichment process.[162] The software then varied the speed at which centrifuge components moved and caused them to break; however, it did so slowly, over time, while feeding false data to human operators who undoubtedly would have turned off the machines had they realized something was amiss.[163] The result was physical damage to machines caused by a cyberspace operation.

Stuxnet operated under Iranian noses for some time. In fact, they appear to have been none the wiser until after Stuxnet got out into the "wild" (the Internet) and a private security company discovered the malicious software on a client's systems.[164] The Iranian government initially refused to admit anything had happened.[165] When they eventually did admit a cyberspace operation had caused damage, the Iranians blamed the United States and Israel[166] while downplaying Stuxnet's impact and announcing it would build its own cyberspace capabilities.[167] What the Iranians did not do is complain to the UN Security Council

that Stuxnet was a use of force, an act of aggression, or breach of the peace, or seek condemnation of the operation in the UN General Assembly.[168] Nor, for that matter, did Iranian leaders or their allies use terms like "act of war," "use of force," "armed attack," or "act of aggression." Instead, it was silence followed by vengeful rhetoric and development of the very same capabilities that damaged their equipment.

This lack of Article 2(4)-centered protest is particularly telling given that Iran is hardly a shrinking violet on the international stage. On the contrary, Iran has initiated ICJ proceedings against the United States on four occasions since 1988, with the last filed in 2018.[169] Furthermore, Stuxnet specifically targeted Iran's nuclear enrichment program, which Iran maintained was a peaceful pursuit of nuclear energy to which it had an "inalienable right" under the Non-Proliferation Treaty.[170] Muted state response to cyberspace operations is not unusual, but in this scenario, one could justifiably expect greater protestations in at least the international press. The furthest Iran was willing to go to was to call itself the "target of sabotage."[171] In the international legal system where exact phrasing from governments matters a great deal, this is notably not "use of force" or "act of aggression" or some other phrase that is meaningful to the modern *jus ad bellum*.

Iran's response to Stuxnet may seem puzzling.[172] The operation did, after all, cause physical damage to their enrichment equipment. Upon closer examination, however, the absence of Article 2(4) rhetoric makes sense given how the physical damage was brought about. Stuxnet was a complicated operation, requiring complex code for the software, extensive intelligence, and even figuring out how to infect the facility's internal network despite it being sealed off from outside networks.[173] In addition to the general complexity of operations, Stuxnet was also intricate in execution. It did not barge (to the extent software can barge) into a control system and begin wreaking havoc. Instead, it slowly and surreptitiously manipulated a control system in ways that exceeded component tolerances, which in turn "caus[ed] the machines to wear out and break."[174] It managed to do this while keeping human operators in the blind so that they did not interfere with the operation.

Stated simply, Stuxnet did not act like a form of conventional armed force. It acted like a complicated espionage and sabotage operation that "ultimately depend[ed] on human operators to make key, damaging decisions based on their assessment of manipulated information."[175] It did not send data to a machine in order to hijack the machine's internal power and damage or destroy it in a manner that resembles a form of armed force. Rather, it sent data to human operators to dupe them into not interfering with gradual, incremental damage to their equipment. This difference in the operational process makes all the legal difference.

Consider Stuxnet through the lens of the electronic warfare-cyberspace operations analogy. Relevant electronic warfare capabilities[176] can use pulses of electromagnetic energy to overheat and permanently damage circuitry, or jam, overpower and misdirect the processing in computerized systems.[177] As networked systems with complex computerized machinery, Iran's enrichment program could have been targeted by electronic warfare. However, while capable of destroying or interrupting the function of the centrifuges, electronic warfare cannot act like Stuxnet. To be sure, an aerial platform might have to fool human radar operators in order to get close enough to use its electronic warfare capability, but once there the method used would act like a weapon employing armed force. This is decidedly not how Stuxnet operated. Accordingly, Stuxnet would not have been a use of force under the electronic warfare-cyberspace operations analogy.

That the electronic warfare-cyberspace operations analogy would result in a finding of non-force in these case studies is not by itself significant. What gives these results substantial weight is that it is in line with Iran's response to Stuxnet and Estonia and NATO's response to the Estonian DDoS attack, which is another way of saying that it comports with state action interpreting Article 2(4) in the cyberspace operations context. Had Stuxnet in particular inflicted its damage through a form of electronic warfare that can be considered a use of force, or through a cyberspace operation closely resembling one, Iran's response may well have been different and the world might be discussing Stuxnet in a different light.

It is admittedly difficult to form definitive conclusions from two case studies as to what Article 2(4) means in the cyberspace operations context. Nevertheless, what state action there is indicates that "most, if not all, documented cyber action taken by states to date have fallen below the 'use of force' threshold."[178] Moreover, if the work of the cumbersomely named UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE) is any indication, certain states—including Russia and China—are hesitant to concede the militarization of cyberspace.[179] This position is unsurprising given that Russian doctrine defines cyberspace operations as information warfare rather than as cyberwarfare. Under this view, cyberspace operations are a way to use and manipulate information to meet political objectives *without* using military force, or, if conventional military force is unavoidable, to shape world opinion in a way that is favorable to Russia's physical world use of force.[180] Either way, it is clear that the Russian perception of military force is decidedly conventional; it does not appear to include cyberspace operations at all. China has taken a similar tone as Russia, acknowledging that the UN Charter applies to cyberspace operations but also asserting that the use of force bar should be a high one.[181] Even the United States, perhaps the most overtly bellicose of nations in

the cyberspace context,[182] has focused of late on the role of cyberspace operations in "continuous competition" between states, though it does not absolutely rule out more belligerent activities.[183]

The work of the GGE and reports of Russian and Chinese viewpoints suggest that many states, though they recognize international law's applicability, do not wish to associate cyberspace operations with the concept of force and everything that term implies in the UN Charter context. This attempt at disassociation is undoubtedly due, at least in part, to a desire to preserve maneuver space. However, given the expressed intent to remain short of the Article 2(4) threshold, it also suggests the world will see more of the same cyberspace operations it is already seeing: lots of data targeting data and data targeting human thought and behavior. Additionally, it suggests that some of the most cyber active states in the world view Stuxnet in the same manner as the Iranians appear to have—as a highly complex sabotage operation executed in a manner short of a use of force.

These combined factors indicate that further clarification from state action is unlikely to be forthcoming, which adds tremendous weight to available state action and makes Iran's response to Stuxnet particularly consequential. When a state like Iran has been the victim of what might be a breach of international law and chooses to discuss it in every way other than as a use of force and then develops the same type of capabilities, its silence on the point suggests political tolerance if not a belief in the act's legality.[184] Consequently, Iran's silence on Article 2(4) is nothing short of deafening. Available state action thus indicates that the method employed still matters even in cyberspace operations, which in turn suggests that analogical tools analyzing such cases must be capable of accounting for both means and effects of state action. Trends in state action, once again, exhibit the wisdom of the electronic warfare-cyberspace operations analogy.

V. Principles of Application

The foregoing analysis makes the case for the electronic warfare-cyberspace operations analogy by demonstrating the great similarity of the comparators and the sensibility of its adoption. While the analogy itself is the focus of this article, this exposition would be incomplete without some attention to how the model could be employed. What follows are three guiding principles—analytical presumptions, really—that form a starting point for analyzing the Article 2(4) permissibility of a cyberspace operation. As will hopefully be plain to the reader, the principles are based in concepts introduced in Part III, namely, that cyberspace operations should be categorized based on what they target: the mind, data alone, or machines.

A. Guiding Principles

Principle #1.
A cyberspace operation that targets machines is presumptively a use of force in violation of Article 2(4) if it closely resembles an electronic warfare use of force.

Principle #2.
A cyberspace operation that targets human thought and seeks to influence behavior is presumptively not a use of force in violation of Article 2(4).

Principle #3.
A cyberspace operation that targets data alone is presumptively not a use of force in violation of Article 2(4).

Generally speaking, Principle #2 includes acts akin to political and economic coercion that states have practiced against each other since time immemorial, and which have never been a violation of Article 2(4). Principle #3 includes acts akin to information exploitation and espionage, which, again, are not violations of Article 2(4). Finally, Principle #1 captures the heart of the matter: cyberspace operations that so closely resemble a form of armed force that crossing the Article 2(4) threshold is possible. Notably, if one accepts a *de minimis* force threshold for Article 2(4), analysis under Principle #3 will require determining whether the operation remains within that body of tolerated actions.

In applying these principles, it is important to remember that they are presumptions. A policy may restrict cyberspace operations in ways that the law would not. Additionally, an operation that combines two or more principles might warrant treatment as a use of force if it skews to the closely-resembles-armed-force side of the spectrum. Ultimately, the framework is useful as an analytical starting point from which in-depth Article 2(4) analysis can proceed.

B. Critique and Response

The electronic warfare-cyberspace operations analogy and its guiding principles will, no doubt, have its detractors. Among possible criticisms, claims of imprecise categorization in Principles #2 and #3 are perhaps likely. It is helpful here to remember that *similarity*, not identicality, is the key to good legal analogy.[185] That a cyberspace operation does not look precisely like espionage or exactly like economic or political coercion does not prevent its cate-

gorization as such.[186] Indeed, whether every cyberspace operation fits neatly into Principle #2 or Principle #3 is immaterial to the *jus ad bellum*. Whether resembling cyberspace-based election meddling or old-fashioned theft, the point is that cyberspace operations in Principles #2 & #3 do not fit and should not be shoehorned into Principle #1. On this point, it is worth noting that as far back as the Hague Convention (II) the great powers of the world began disabusing themselves of the notion that war is a justifiable response to economic harms, [187] a position further solidified when economic coercion was left out of Article 2(4)'s prohibition on the use or threat of force.[188]

The most likely criticism of the electronic warfare-cyberspace operations analogy is that Principle #1 is underinclusive. For instance, how could opening the gates of a dam and killing thousands of people with a wall of water not be a use of force even if the means of operation is not analogous to electronic warfare? In response, it should be acknowledged that if a cyberspace operation bears enough of the factors usually associated with a use of force or an armed attack, it probably should be considered a violation of Article 2(4). In other words, some effects may be so bombastic that being analogous to electronic warfare is unnecessary. This concession may seem like an abandonment of the analogy. However, it merely recognizes that no analogy is so good that it works in every possible scenario. Moreover, at the high end of the scale, calling a cyberspace operation a use of force and possibly responding with armed force is ultimately a political decision.[189] Under a political calculus, a really, really devastating cyberspace operation may produce an Article 2(4)-laced response regardless of the legal analysis used.

More importantly, the purpose of the electronic warfare-cyberspace operations analogy is not to consider the worst possible thing that might happen, but rather to account for the world as it actually is. Headlines have for years been full of dire cyberspace predictions,[190] and treatment by international law scholars has largely been the same, providing exemplars for analysis like disabling an air traffic control tower and causing an airliner to crash;[191] causing a dam to open;[192] and shutting down a power grid resulting in deaths and millions of dollars lost.[193] With examples like these, it is little wonder the effects model has gained a majority following in western states. However, nothing approaching the above examples has occurred. Indeed, in the years since state cyberspace operations began, instead of cyber death and destruction the world has experienced rampant data theft,[194] espionage,[195] and political influence operations.[196] As one commentator notes, in the realm of operations states are actually conducting, catastrophe is possible but decidedly unlikely outside of an armed conflict.[197]

Briefly consider why this might be. First, as already mentioned, cyberspace operations are limited in what they can achieve. Taking down a power grid would undoubtedly be inconvenient and may even result in death. However, it is imminently reversible, and unless followed closely by aircraft, tanks, and infantry—i.e., an armed conflict—such operations are unlikely to do anything but anger the victim state into some form of unfriendly response.[198] Furthermore, cyberspace operations work best when they are low key and the identity of the actors is ambiguous.[199] A catastrophic cyberspace operation does not make attribution any easier, but very severe consequences might prompt a state to settle for less definitive evidence when deciding whether the UN Charter's right to self-defense has been triggered.[200] Accordingly, unless prepared to cross the Rubicon of armed conflict, states are likely to stick with cyberspace operations well short of Article 2(4).

Second, cyberspace operations as they are—that is, those well within Principles #2 and #3—have proven sufficient to meet state objectives, which reduces or eliminates the need for more dramatic action.[201] States work incessantly to anticipate who their next adversary is and how that state might be defeated, which includes finding ways to better position themselves and disadvantage the potential enemy. Cyberspace operations, through things like intelligence gathering, information operations, and preparing adversary networks for exploitation excel at this competition stage of conflict.[202] Notably, the measures needed to achieve these objectives do not include blowing up nuclear power plants. Indeed, to be effective, state actions in this context must remain below a threshold that might generate a conventional armed response. Consequently, states have little reason to undertake cyberspace operations that risk missiles flying and carrier battle groups sallying forth.[203] Avoiding conflict in the present explains why, for instance, Russia might infiltrate power grids in the United States but stop short of actual damage.[204] Russia is preparing to exploit vulnerabilities and impose costs in the event a shooting war breaks out; it is not preparing for a standalone cyber war. In the meantime, as long as states like Russia avoid cyberspace operations against the United States that "proximately result in death, injury, or significant destruction," a line state practice suggests even Stuxnet did not cross, the United States is unlikely to treat Russia's actions as a use of force.[205] Given the effectiveness of other, clearly non-force cyberspace operations, why tempt fate?

Third, a catastrophic cyberspace operation is likely to be a Pyrrhic victory at best. Consider the effect of an attack on the United States' financial sector. Such an attack would indeed be costly for the United States and might even send the national economy spiraling. However, it is not as if the largest economy in the world exists in a bubble.[206] In fact, quite the opposite is true. Consequently, a state conducting a catastrophic cyberspace attack against financial systems in the

United States is tantamount to attacking itself. Outside of an actual war, why would a state ever put its economy at such risk?[207]

The simple truth is that a state-to-state catastrophic cyberspace operation has not occurred and is highly unlikely to. Consequently, if crossing the Article 2(4) threshold occurs, it is likely because a state took a slightly too aggressive approach to a particular operation, or an actual armed conflict has or is about to start in which case whether a cyberspace-perpetrated use of force has occurred is moot. Down in the trenches of this reality, what is needed is an analogical model that views Article 2(4) through a nuanced lens capable of distinguishing the minority of operations that are truly a use of force from the great majority which are not, while remaining flexible enough to accommodate the unlikely but horrific results of the very worst cyberspace operations. In providing a bridge between cyberspace and armed force, the electronic warfare-cyberspace operations analogy does exactly this in a way that comports with international law and supports the letter and purpose of the UN Charter framework. Principle #1 is thus not under inclusive; it is precisely inclusive enough.

VI. Effects Model Critiqued

This article proclaimed in its introductory remarks that the effects model's departure from the traditional *jus ad bellum* was a step too far, and the analysis following that declaration has repeatedly asserted the superiority of the electronic warfare-cyberspace operations analogy. Such claims must necessarily be able to demonstrate their veracity, and while the foregoing analysis has made a case for a new analogical model, it has not demonstrated how the effects model falls short. To remedy this analytical gap, this section will subject the effects model to the same analysis which the electronic warfare-cyberspace operations analogy has undergone. The examination begins with the analogy made—effects to effects—and analyzes just how similar the effects of a cyberspace operation and a kinetic or non-kinetic use of force must be to for the effects model to deem the cyberspace version a use of force too. As this analysis will demonstrate, the effects model's similarity requirements are not rigorous, and it readily accepts imprecise comparison as sufficient. The examination then turns to the effects model's attempts to remedy its tendency toward imprecision, and how those attempts are ultimately ineffectual and lead to false equivalence of comparators. The analysis ends with an examination of the broader implications of the effects model's imprecision, with the ultimate conclusion that the electronic-warfare-cyberspace operations analogy is the superior analogical model.

A. Analogical Imprecision

Under the effects model, a cyberspace operation is a use of force if it produces effects analogous to those generated by kinetic or non-kinetic actions that are rightly considered a use of force.[208] If the effects of one are a use of force, it follows that the effects of the other are too. For the kinetic comparison, that might mean an effect similar to that produced by high explosives in artillery shells, missiles, or bombs, or putting a hole in an object as a bullet could. For non-kinetic actions, that might mean effects similar to those created by phosgene, a type of chemical weapon agent that attacks a victim's respiratory tract, and in extreme cases, swells membranes and causes the lungs to fill with liquid resulting in death from lack of oxygen.[209]

At the outset, it should be acknowledged that the effects-to-effects analogy has some merit in the most extreme circumstances. A catastrophic cyberspace operation, the results of which bear all the effects associated with conventional armed force, likely should be characterized as a violation of Article 2(4). For instance, a state cyberspace operation that releases a substance causing victims to "choke and vomit[] as their lungs constrict, then suffer through tormenting muscle spasms and eventual death," probably is a use of force if it can be adequately attributed.[210] However, that kind of cyberspace operation has not materialized and is decidedly unlikely to outside of an armed conflict. For an analogy to be worthwhile, it must be able to parse the subtle distinctions of cyberspace operations as they actually exist. It is here that the effects model falls short.

As the most well-known example, an analysis of Stuxnet helps illustrate this point. Stuxnet damaged Iranian centrifuges by (1) analyzing the industrial control system to find the right controllers, (2) recording normal operations and sending false data to system monitors, and (3) causing internal components of machines to speed up and slow down in a way that caused them to fail at a higher than standard rate over a lengthy period.[211] The operation was so complex and multi-faceted that researchers who analyzed Stuxnet referred to it as having a "sabotage strategy."[212] For Stuxnet to be a use of force, the effects model requires a kinetic or non-kinetic use of force that has analogous effects. The question, then, is what kind of kinetic or non-kinetic action is capable of producing this result?

The short answer is that there are not any. A bullet could pierce the centrifuge and damage internal components, much like a round from a large caliber rifle stops a boat engine.[213] An electronic warfare weapon mounted on an aerial platform could use directed energy to overload electrical circuitry and bring the centrifuge's internal components to a halt.[214] A biological agent like smallpox might make all of the human operators sick and cause the centrifuges to cease

operation through workforce depletion. The point, however, is that these forms of armed force are not capable of causing machine components to subtly wear out too fast over a lengthy period.[215]

Given this dissimilarity, one might expect a finding of no force used. However, effects model proponents seem unequivocal in their view that Stuxnet *was* a use of force.[216] From this result, one must conclude that the effects model does not require true similarity of effects; the fact that Stuxnet caused some type of damage is sufficient, regardless of whether a kinetic or non-kinetic form of armed force can actually produce that result. Stuxnet thus reveals that on the low end of the operational spectrum, where the nations of the world are conducting cyberspace operations, its analogy is imprecise and does not do what it purports to do.

Lest requiring this level of similarity be considered too harsh a standard, it is worth considering how changing the facts of Stuxnet affects the analytical outcome and why the ease of that modification is significant. An effects model proponent might argue that had a cruise missile damaged the centrifuges, the world would certainly consider Stuxnet a use of force.[217] That a cruise missile does not create the same effect is immaterial; damage is damage. While a cruise missile would undoubtedly be a use of force, this example does not settle the issue, for if one side of a debate gets to change the facts to fit a bellicose scenario, the other must be permitted the same revisionist luxury.

Instead of a cruise missile, suppose an intelligence officer recruited an Iranian scientist to reprogram the control system to do precisely what Stuxnet did: cause sensitive components to fail over time while keeping human system monitors in the dark. Convincing a scientist to betray his country would not involve armed force, but rather some means of influencing the scientist's thought and behavior—a scenario which is notably more similar to Stuxnet's actual operational scheme than is the cruise missile example. As this revision reveals, Stuxnet actually has more in common with physical-world human intelligence (a form of espionage) and information operations (akin to political coercion), neither of which implicate Article 2(4), than it does with a form of armed force.[218] Consequently, the fact that damage occurred is not the only factor relevant to determining the legal status of Stuxnet.

The ability to change the analytical outcome of Stuxnet this easily is a tremendous problem for the effects model. Analogy relies on comparing items that are similar, not identical, which means that every analogy will compare items that are dissimilar to some degree. The fact that dissimilarity is built into every analogy means there is always danger of taking the comparison too far by pronouncing

items alike that are not genuinely similar. Indeed, the more an item strays from its comparator, the more likely it is that the item is more similar to something else and, therefore, *is* something else. Unless this slide away from the comparator is arrested, the result is false equivalence of the items compared. Sufficient arrest comes from a firmly rooted comparator and a demand for close similarity of the items compared to it. Only then is an analogy precise enough to mitigate the risk of false equivalence.

Comparing cyberspace operations to a form of armed force like electronic warfare meets this requirement. By using a firmly-rooted form of armed force as a comparator and requiring close resemblance to it, the analogy ensures that cyberspace operations implicating Article 2(4) do not stray far from its analytical rigor. The effects model, on the other hand, purports to be rooted in effects producible by kinetic or non-kinetic armed force, but then fails to demand genuine similarity, relying instead on "effects" in the generic sense of the term. Such imprecision does not make for a strong analogical model. Instead, it is a recipe for false equivalence, which, as slightly changing the facts of Stuxnet demonstrates, leads to incorrectly labelling cyberspace operations as uses of force when they actually bear closer resemblance to state actions that do not implicate the *jus ad bellum*. The ultimate result is treating *dissimilar* items similarly or similar items similarly by happenstance, which is the definition of a poor analogy.

B. Attempts to Avoid False Equivalence

The effects model attempts to remediate this imprecision in two ways. Its first attempt is through an analogical hook intended to close the gap between cyberspace operations and armed force. While the tenets of the effects model are recorded in the Tallinn Manuals, it origins can be found in a law review article written by Professor Michael Schmitt nearly fifteen years before Tallinn 1.0's publishing.[219] One of the article's conclusions is that Article 2(4) encompasses more than armed force,[220] and in taking this position, the article placed Article 2(4)'s prohibitive line somewhere between armed force and economic and political coercion.[221] However, this expansion was undertaken with a strict caveat. According to the article, it is necessary for Article 2(4)'s scope to widen, but in order to remain within the UN Charter framework, the expansion must remain rooted in the traditional, armed force-focused analysis. Analogizing the effects of cyberspace operations to the effects of kinetic or non-kinetic armed force is the hook that keeps Article 2(4) from expanding so much that the entire concept of force changes.[222]

As Stuxnet demonstrates, however, actually applying the analogical hook is highly problematic. This difficulty may not matter so much on the very severe end of things; a massive explosion is still a massive explosion, after all. But on the low end of cyberspace operations, where states of the world are operating, the effects model settles for a comparison that is, at best, sort of similar. Indeed, real world application suggests that the analogical hook connecting effects to armed force is hanging loosely, if at all, which means there is little to prevent further expansion of Article 2(4) to facilitate an approach focused solely on adverse consequences.[223] As Professor Schmitt suggested those many years ago, such an expansion means a new concept of force that exists outside of the UN Charter framework.[224]

The effects model's second attempt at remediation is through a factor test designed to skew Article 2(4) closer to armed force than to economic or political coercion, neither of which can violate Article 2(4).[225] However, these factors are not legal criteria,[226] and more importantly, are highly malleable. Indeed, as one author noted, the criteria are "illuminating," but so broad that different viewers can arrive at opposite conclusions on the legal status of a given cyberspace operation.[227] The 2007 DDoS attack on Estonia is an apt example. Leading proponents of the effects model appear to have concluded that the DDoS attack was not a use of force.[228] However, exactly why that conclusion is drawn is not readily apparent. The Estonian government was greatly affected by the DDoS attack and it cost the economy millions of dollars, which gives it the appearance of an attack that is both severe and measurable.[229] Furthermore, the attack kicked off within hours of the Soviet statue's removal, which suggests immediacy, and persisted for three weeks thus further indicating its severity. Moreover, the DDoS attack was direct in that the method of attack (increased network traffic) forms a direct link from individual attackers or botnet machines to the information systems ultimately affected. Given these combined factors, and assuming the attack was correctly attributed to the Russian state, why would the DDoS attack not be a use of force?

Under the electronic warfare-cyberspace operations analogy, the Estonian DDoS attack was not a use of force because it is akin to political coercion aimed at Estonians and their government. In other words, data targeting human minds. Moreover, the attack closely resembled forms of electronic warfare that are not uses of armed force. Analysis under the effects model and its factors is much less concrete and, as the analysis above suggests, lends itself to different analytical results with no way of determining which position is correct. The effects model's potential for equally valid yet diametrically opposed conclusions is further demonstrated by the Stuxnet-based hypotheticals (cruise missile and Iranian turncoat) posed earlier. When the viewer gets to decide the content of the standard and then applies the facts of a cyberspace operation to that standard, the result will naturally reflect that

viewer's preference. Consequently, the factors do little to tighten the effects model's imprecision, which means it does little to remediate the risk of false equivalence.

C. Implications of Imprecision

Consider the broader implications of this inability to arrest the false equivalence slide. First, the effects model's imprecision demonstrates its incongruity with trends in state action. As previously detailed, Iran's lack of Article 2(4)-tinged rhetoric following Stuxnet suggests that whatever a cyberspace-perpetrated use of force looks like, it is something different than Stuxnet. Further, indices from the Russians and Chinese suggest those nations view "force" in terms of conventional armed force and intend to maintain their cyberspace activities well short of it. In this scenario, Iran's demure reaction to Stuxnet looms large. In a legal system heavily dependent on what states do and say, the imprecision of the effects model and its incongruence with trends in state action is highly problematic.

Second, the effects model's imprecision provides inconsistent analytical results. As previously mentioned, the analogical hook intended to prevent cyberspace operations from straying too far from armed force is very loosely connected. With the hook weakened and the factor test doing little to strengthen it, there is scarcely a reason not to expand Article 2(4) into an approach focused purely on adverse consequences.[230] Notably, however, no matter how broadly Article 2(4) is interpreted, it will never include economic and political coercion or espionage regardless of how severe the effects may be. This combination of factors results in a consequences-focused model in which the effects of an operation are all that matters unless it is not all that matters (economic and political coercion and espionage), in which case the modality matters too, but there is no good way to tell the difference.

Third, and most importantly, the effects model's imprecision undermines the larger UN Charter framework in which Article 2(4) resides. As discussed previously, placing the Article 2(4) threshold at armed force bars the small actions that lead to wider conflict, while also not prohibiting so much that a broader conflict paradoxically results from states too easily invoking the right to self-defense. Focusing on adverse consequences irrespective of their similarity to armed force threatens this dynamic by expanding the scope of Article 2(4) well beyond its normal limits.[231] In short, it makes too much illegal and provides a ready-made excuse for aggressive states to invoke Article 51.

There are signs the effects model already extends this far and has arguably never insisted upon results that very closely resemble the effects of kinetic or non-kinetic armed force; operations that meet these criteria are simply the easiest ones to categorize.[232] Moreover, since this initial hard-wiring, the effects model's tolerance of imprecision seems to have increased. In a recent article, Professor Tobias Kliem observed a remarkable difference between Tallinn 1.0, published in 2013, and its successor, published in 2017.[233] More specifically, while Tallinn 1.0 categorically excluded economic and political coercion from the ambit of Article 2(4),[234] this language is noticeably missing from the correlating portion of Tallinn 2.0.[235] To be sure, Tallinn 2.0 acknowledges that economic and political coercion are not uses of force; however, the assertion is not as robust as it was in the previous version.[236] Additionally, while Tallinn 1.0's exclusion included cyberspace operations "otherwise analogous to" economic or political coercion, Tallinn 2.0 takes no such position.[237]

This distinction between editions is subtle but significant. The softer and narrower language of Tallinn 2.0 suggests that under the effects model, the categories of economic and political coercion now include fewer actions than before, which means Article 2(4) must include more than ever. This difference reveals a trend toward a comparison concerned only with adverse consequences that relegates similarity to the effects of armed force to happy coincidence instead of the foundation of the analogy.[238] The armed force "sweet spot" formerly occupied by Article 2(4) is nowhere to be seen in this approach. As Professor Jack Beard has noted, focusing solely upon adverse consequences leads to chasing "legal phantoms" in cyberspace, which are "situations in which numerous policy questions, domestic criminal issues, and technological challenges are misinterpreted as legal problems … that implicate the *jus ad bellum*." [239] The natural response to these legal phantoms is to make Article 2(4) more inclusive in order to capture what are unarguably damaging state actions. However, the ubiquity of such operations suggests this is a mistake. To broaden the *jus ad bellum* analysis beyond a close analogy to armed force is to "diminish restrictions on the use of force, thereby significantly weakening key safeguards upon which the international community relies …."[240] Consequently, in addition to the risk of false equivalence, the imprecision of the effects model is a genuine threat to the middle ground of Article 2(4) and ultimately to the international peace and security the UN Charter seeks to protect.

This expansive trend is no doubt rooted in a desire to reduce the number of harmful cyberspace operations. Though this is a laudable goal, Article 2(4) is not the right vehicle for its pursuit. Remediating the risk of imprecision posed by the effects model and avoiding an analytical slide into methods focused purely on negative consequences lies in adhering as closely as possible to the traditional,

armed force-focused approach to the *jus ad bellum*. Expository analysis of the effects model reveals its inability to do so, something that might be tolerable if the effects model were the only analogical option available—but it's not. By comparison, the electronic warfare-cyberspace operations analogy uses great similarity between comparators and a key difference between to create a precise comparison that holds fast to the traditional *jus ad bellum*. The effects model's analogical weaknesses are therefore the electronic warfare-cyberspace operations analogy's strengths, which, in the end, makes it the better analogical approach for judging the *jus ad bellum*-compliance of state cyberspace operations.

VII. Concluding Thoughts

In the end, the effects-based approach of the Tallinn Manuals is a broad-brush analogy that is overly inclusive and abandons the means-based *jus ad bellum* in the face of legal principles and state action that suggests modality of state action still matters. Moreover, despite efforts to tighten its analogy, the effects model remains imprecise, which risks labelling as uses of force state actions that more closely resemble physical world measures that do not implicate the *jus ad bellum.* The result is an imprecise analogy that risks treating dissimilar cases similarly, which is the opposite of what an analogical model is supposed to do.[241]

The electronic warfare-cyberspace operations comparison avoids the pitfalls of the effects model by analogizing cyberspace operations to an actual form of armed force rather than settling for a generic comparison of effects. Electronic warfare and cyberspace operations are similar in how they work, how they are used, and even in their limitations, which suggests the two can be gainfully analogized for *jus ad bellum* purposes. Moreover, careful analysis of the UN Charter's text, purpose and subsequent interpretation, not to mention state practice in the cyberspace operations context, demonstrate that Article 2(4)'s prohibition on the use of force remain closely tethered, even in cyberspace operations, to the concept of armed force. In other words, the traditional approach—that the means used to conduct the operation matters a great deal—is as applicable to cyberspace operations as it is to any other form of state action.

This, in turn, establishes that the methods used in state cyberspace operations are as vital to the use of force analysis—and arguably more so—as the effects the operation creates. Consequently, any analogical model seeking to reconcile cyberspace operations and the *jus ad bellum* must be capable of accounting for both means and effects. Electronic warfare enables such an analysis by forming an analogical bridge between cyberspace operations and armed force that is at most a slight expansion of the traditional approach. If adherence to the *jus ad bellum* framework is more

desirable than its undermining (and it is), legal analysis capable of such precision is not merely advantageous but genuinely imperative. As examination of the effects model makes plain, the electronic warfare-cyberspace operations analogy is the more precise and thus the better option.

Nevertheless, much work remains. By requiring close analogy to a form of armed force and thereby retaining the use of force threshold at its original sweet spot, the comparison will likely result in shrinking the group of Article 2(4)-threatening cyberspace operations. Notably, this will not change the damaging nature of such non-force actions, which begs the question of what to do with them. It will require a shift in focus from armed force, which is generally military-centric, to one of cybersecurity reinforced by international norms of acceptable state conduct. Over time, this may even lead to a cyberspace-specific area of international law as some have suggested is needed.[242] In the meantime, the work can proceed with cyberspace operations implicating Article 2(4) firmly ensconced where they belong—in close analogy to a form of armed force.

Endnotes

[1] Int'l. Comm. of the Red Cross, *International Humanitarian Law: Answers to Your Questions*, 8 (2015), https://www.icrc.org/en/publication/0703-international-humanitarian-law-answers-your-questions.

[2] U.N. Charter art. 2(4).

[3] The White House, *International Strategy for Cyberspace*, 14 (May 2011) ("When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country …. We reserve the right to use all necessary means—diplomatic, informational, military, and economic—as appropriate and consistent with applicable international law, in order to defend our Nation, our allies, our partners, and our interests."); *see also*, The White House, *National Cyber Strategy of the United States of America*, 21 (Sept. 2018) ("All instruments of national power are available to prevent, respond to, and deter malicious cyber activity against the United States. This includes diplomatic, information, military (both kinetic and cyber), financial, intelligence, public attribution, and law enforcement capabilities.").

[4] *See generally*, Tallinn Manual on the Int'l Law Applicable to Cyber Warfare 48 (Michael N. Schmitt ed., 2013); *see also*, Tallinn Manual 2.0 on the Int'l Law Applicable to Cyber Operations 331 (Michael Schmitt ed., 2d ed., 2017) (hereinafter Tallinn 1.0 and Tallinn 2.0, respectively, or Tallinn or Tallinn Manuals collectively).

[5] Johann-Christoph Woltag, *Cyber Warfare*, Max Planck Encyclopedia of Public International Law (2015) (Paragraph 8 reflects that the effects model is the majority view).

[6] *See* Tallinn 1.0, *supra* note 4, 48.

[7] Mary Ellen O'Connell, *Preserving the Peace: The Continuing Ban on War Between States*, 38 Calif. W. Int'l L.J. 41-42 (2008).

[8] Yoram Dinstein, War, Aggression, and Self-Defence 176 (4th ed., 2005). Wars of this period generally followed a totalistic model, meaning large national armies with few restrictions on how they fought one another. *See also*, James Turner Johnson, Ethics and the Use of Force: Just War in Historical Perspective 39 (2011).

[9] *See* Johnson, *supra* note 8, 39.

[10] Machine guns, repeating small arms, advanced artillery, modern-style naval vessels, and aircraft, to name a few. *See* Johnson, *supra* note 8, 39.

[11] Hague Convention Respecting the Limitation of Employment of Force for Recovery of Contract Debts (Hague II), art. 1, Oct. 18, 1907, 36 Stat. 2241, 1 Bevans 607. ("The Contracting Powers agree not to have recourse to armed force for the recovery of contract debts claimed from the Government of one country by the Government of another country as being due to its nationals.") (hereinafter Hague (II) 1907).

[12] League of Nations Covenant, art. 11.

[13] Renunciation of War as an Instrument of National Policy (Kellogg-Briand Peace Pact or Pact of Paris), art. 1, Aug. 27, 1928, 46 Stat. 2343, 94 L.N.T.S. 57.

[14] In a period in which states still formally declared war on each other, a state could ostensibly avoid triggering the terms of international agreements by waging an "imperfect," undeclared war on its adversary. *See* Catherine Lotrionte*, Reconsidering the Consequences for State-Sponsored Hostile Cyber Operations Under International Law*, The Cyber Defense Review, 73, 77 (Summer 2018). For an example of "imperfect" war, *see generally*, *Bas v. Tingy*, 4 U.S. 37 (1800).

[15] O'Connell, *supra* note 7, 45 ("The Axis powers made self-defense claims when justifying their actions: Germany claimed the need for *Lebensraum* (living space), and Japan claimed the need for access to natural resources."). Guarding against the expansive use of self-defense by international agreements is perhaps why Common Article 2 of the Geneva Conventions of 1949 expressly states that an international armed conflict exists anytime there is a declared war or an armed conflict between states "even if the state of war is not recognized by one of them," thus relying on the fact of belligerency rather than nomenclature when determining whether an international armed conflict is in progress. *See*, *e.g*., Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, Aug. 12, 1949, 6 UST 3114; 75 UNTS 31.

[16] United Nations Audiovisual Library, *San Francisco 1945*, https://www.unmultimedia.org/avlibrary/asset/1288/1288630/ (last visited Mar. 29, 2019).

[17] *Growth in United Nations Membership, 1945-Present*, https://www.un.org/en/about-us/growth-in-un-membership (last visited Mar. 19, 2021).

[18] U.N. Charter, art. 2(4) (emphasis added).

[19] *Id*. at art. 51.

[20] *Id*. at art. 37, 51.

[21] Notably, customary international law also prohibits the use or threat of force. However, the UN Charter's provisions predominate the modern *jus ad bellum* calculus, and consequently, it is this article's primary focus. O'Connell, *supra* note 7, 41 ("Both the general prohibition of the use of inter-State force and the exception to it (the right of self-defence) are part and parcel of customary international law, as well as the law of the Charter.").

[22] The decades since UN Charter enactment have seen many examples of small-scale uses of force for which states have demonstrated tolerance. For accounts of U.S. reconnaissance aircraft violating Soviet airspace s*ee* Evan Thomas, Ike's Bluff: President Eisenhower's Secret Battle to Save the World 365-379 (2012), and Ben R. Rich & Leo Janos, Skunk Works 137-168 (1994). For an account of *sub rosa* submarine warfare between the U.S. and the Soviet Union, *see* Sherry Sontag et al., Blind Man's Bluff: The Untold Story of American Submarine Espionage (1998). For a more complete listing of small-scale uses of force tolerated by the international community *see* Michael W. Reisman, *Criteria for the Lawful Use of Force in International Law*, 10 Yale J. Int'l L., 279, 281 (1985).

[23] Oona A. Hathaway & Rebecca Crootof, *The Law of Cyber-Attack*, 100 Cal. L. Rev., 817, 843 (2012); *see also*, Jason Barkham, *Information Warfare and International Law on the Use of Force*, 34 N.Y.U. J. Int'l L. & Pol. 57, 72 (2001) (observing that "armed force" includes both kinetic and non-kinetic forms).

[24] Jack M. Beard, *Legal Phantoms in Cyberspace: The Problematic Status of Information as a Weapon and a Target Under International Humanitarian Law*, 47 Vanderbilt Journal of Transnational Law, 67, 99 (2014); *see also*, Tallinn 1.0, *supra* note 4, 46 ("Accordingly, whatever 'force' may be, it is not mere economic or political coercion. Cyber operations that involve, or are otherwise analogous to, these coercive activities are definitely not prohibited uses of force.").

[25] Duncan B. Hollis, *Why States Need an International Law for Information Operations*, 11 L&C L. Rev., 1024, 1041 (2007).

[26] *Id*.

[27] *Id*.

[28] Tallinn 1.0, *supra* note 4, 50.

[29] TALLINN 1.0, *supra* note 4, 46.

[30] Woltag, *supra* note 5.

[31] TALLINN 1.0, *supra* note 4, 45.

[32] TALLINN 1.0, *supra* note 4, 48.

[33] Martha Minnow, *How Reasoning By Analogy Works in Law*, The Bridge: Analogy & Precedent, https://cyber.harvard.edu/bridge/Analogy/analogy3.htm (last visited Mar. 25, 2019).

[34] *Id*.

[35] *Id*. (emphasis added).

[36] *See* Hollis, *supra* note 25, 1031 ("[Computer network operations] incorporates an offensive and a defensive element: (i) 'computer network attacks' (CNA) that use data streams to deceive, disable, degrade, or destroy adversary computer systems or the infrastructure they support, and (ii) 'computer network defense' that defends against an adversary's CNA.").

[37] U.S. DEPT. OF DEF. & JOINT CHIEFS OF STAFF, ELECTRONIC WARFARE JOINT PUBLICATION 3-13.1, I-1 (Feb. 2012) (hereinafter JP 3-13.1).

[38] U.S. DEP'T OF DEFENSE, DOD DICTIONARY OF MILITARY AND ASSOCIATED TERMS, 78 (Feb. 2019), https://www.jcs.mil/Doctrine/ (hereinafter DoD Dictionary).

[39] U.S. DEPT. OF DEF. & JOINT CHIEFS OF STAFF, CYBERSPACE OPERATIONS JOINT PUBLICATION 3-12, I-4 (June 2018) (hereinafter JP 3-12).

[40] *Id*. at I-1.

[41] A notable exception is the HARM anti-radiation missile, which is often included as a form of electronic warfare because it targets radar systems, such as those used in air defense systems. *See* JP 3-13.1, *supra* note 37, I-4; *see also*, Robert Johnson & Geoffrey Ingersoll, *America's Scariest Electronic Weapons*, Business Insider (Sept. 14, 2012, 9:04 PM), https://www.businessinsider.com/electronic-warfare-weapons-2012-3 (last visited Mar. 29, 2019).

[42] Merriam-Webster Dictionary, https://www.merriam-webster.com/dictionary/kinetic (last visited Feb. 9, 2019).

[43] *See* U.S. Dep't of the Air Force, Air Force Doctrine Document Glossary (March 1, 2021), https://www.doctrine.af.mil/Glossaries/Air-Force-Glossary/ (last visited Mar. 18, 2021).

[44] *See* John Tatum, *HPM DEWs and Their Effects on Electronic Targets*, DSIAC Journal, July 28, 2017, at 33, 36-37.

[45] Jamming and intrusion techniques can be used to deny use of the EMS. *See* JP 3-13.1, *supra* note 37, I-8; AND U.S. ARMY CYBERSPACE AND ELECTRONIC WARFARE OPERATIONS FIELD MANUAL NO. 3-12, 1-28 (Apr. 2017) (hereinafter FM 3-12). Cyberspace operations can achieve the same effect by denying, degrading, or destroying the functionality of information systems and networks upon which they rely. *See* JP 3-12, *supra* note 39, II-7.

[46] *See* JP 3-13.1, *supra* note 37, I-7; *see also*, FM 3-12, *supra* note 45, 1-27.

[47] Electronic warfare can probe a device or system with electromagnetic energy in order to learn its capabilities and how it functions. *See* DoD Dictionary, *supra* note 38, 77. Cyberspace operations can also map networks, find, copy, and manipulate data files, and determine the location of critical components and how they function. *See* JP 3-12, *supra* note 39, II-6.

[48] *See* JP 3-12, *supra* note 39, II-7; JP 3-13.1, *supra* note 37, I-4; and FM 3-12, *supra* note 45, 1-26. *See also*, Clay Wilson, Cong. Research Serv., RL31787, *Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues*, 6 (June 5, 2007) ("Directed energy weapons amplify, or disrupt, the power of an electromagnetic field by projecting enough energy to overheat and permanently damage circuitry, or jam, overpower, and misdirect the processing in computerized systems.").

[49] *See* JP 3-13.1, *supra* note 37, I-4 to I-6; *see also*, JP 3-12, *supra* note 39, II-4 to II-5.

[50] *See* JP 3-13.1, *supra* note 37, I-15 ("Wired and wireless networks continue to evolve, and mobile computing devices continue to grow in both capability and number …. Since cyberspace requires both wired and wireless links to transport information, both offensive and defensive cyberspace operations may require use of the EMS for the enabling of effects in cyberspace.").

[51] Mickey Batson & Matthew Labert, *Expanding the Non-Kinetic Warfare Arsenal*, Proceedings Magazine, Jan. 2012, at 40, 41-42.

[52] Robert Smith, *Maneuver at Lightspeed: Electromagnetic Spectrum as a Domain*, Over the Horizon Journal (Nov. 5, 2018), https://othjournal.com/2018/11/05/maneuver-at-lightspeed-electromagnetic-spectrum-as-a-domain/ ("Both free space and wired networks rely on Maxwell's equations describing electric and magnetic fields whether a computer is connected to the network or not. Cyberspace is simply one way to utilize both wired and free space networks."); *see also*, Forrest B. Hare, *Five Myths of Cyberspace and Cyberpower*, Signal Magazine (June 2007), https://www.afcea.org/content/five-myths-cyberspace-and-cyberpower (last visited Apr. 1, 2019) ("In the cyberspace domain, the electromagnetic spectrum is the maneuver space also governed by laws of physics. That domain is a physically manifested space with closed/wired segments as well as free-space segments …. Cyberspace should be recognized as a physical domain, occurring any place where the electromagnetic spectrum and electronic systems interlink.").

[53] Batson & Labert, *supra* note 51, 41, 42 ("Although it is true that computer networks do help in navigating cyberspace, they are simply tools and not the environment itself. Fundamentally, we are talking about information/data traveling through the spectrum.").

[54] For instance, a cyberspace operation might be used to disrupt an adversary's operations on wired networks in order to force the adversary onto wireless networks that are vulnerable to electronic warfare. Conversely, electronic warfare methods may be used to create EMS conditions that are ideal for a cyberspace operation. *See* JP 3-13.1, *supra* note 37, I-15.

[55] For a side by side comparison of cyberspace and electronic warfare capabilities, *see* Batson & Labert, *supra* note 51, 42 ("For example, consider the following list of EA capabilities: manipulate[ing] their [adversary] radar to show false images; [using] directed electromagnetic energy that, in short pulses, may permanently disable enemy computer circuitry; confusing or misleading an adversary manipulates the adversary's decision loop, making it difficult to establish an accurate perception of objective reality. Looking through a different lens, one could consider the non-kinetic effects here equivalent to a 'cyber effect.' Examine the list again in general terms of more traditionally accepted OCO effects to include just some common examples[:] inserting false data; permanently erasing data; causing irrevocable damage to a network system; modifying routing tables/network addresses; denial of service (DOS) and distributed denial of service (DDOS)").

[56] Thomas Rid, *Cyber War Will Not Take Place*, The Journal of Strategic Studies, Feb. 2012, at 5, 16 (an attack known as "Operation Orchard").

[57] *Id*.

[58] *Id*.

[59] Richard Clarke & Robert Knake, Cyber War: The Next Threat to National Security and What to do About It 1-11 (2010).

[60] Wilson, *supra* note 48, at 6.

[61] Andy Greenberg, *Hackers Remotely Kill a Jeep on the Highway – With Me in It*, Wired (July 21, 2015, 6:00 AM), https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ (last visited Feb. 15, 2019).

[62] *Id*.

[63] *Id*.

[64] Kyle Mizokami, *High-Powered Microwave Ray Gun Can Stall Cars, Trucks*, Popular Mechanics (Apr. 26, 2018), https://www.popularmechanics.com/military/weapons/a20063831/high-powered-microwave-ray-gun-can-stall-cars-trucks/ (last visited Jan. 4, 2019).

[65] Martin C. Libicki, *The Specter of Non-Obvious Warfare*, Strategic Studies Quarterly, Sep. 3, 2012, at 88, 89 (hereinafter Libicki, *Specter*) ("Ambiguity is the heart of non-obviousness. If the victim is unsure of who carried out an operation, it may hesitate to respond in the same way as if it were certain. Alternatively, the rest of the world might have doubts even if the victim is certain, leaving the victim wary of responding as it might have if others were very sure of matters.").

[66] *Id*. at 90.

[67] *Id*. ("Some forms of warfare are non-obvious because the relationship between the attacker and a state is unclear … [i]n some cases the perpetrators may be state employees that are not necessarily, or at least not provably, working under the command and control of the state itself.").

[68] *Id*. at 89.

[69] *Id*.

[70] Beard, *supra* note 24, 132.

[71] For an interesting account of the physical existence of the Internet, *see generally*, Andrew Blum, Tubes: A Journey to the Center of the Internet (2012).

[72] Martin C. Libicki, Conquest in Cyberspace: National Security and Information Warfare 8 (2007).

[73] *Id*. at 8-9.

[74] *Id*.

[75] Beard, *supra* note 24, 98 ("As noted, however, the historic focus in the IHL regime has been on physical forces and objects, which has always included a smaller subset of various nonkinetic, physical weapons, ranging from older versions, such as poison and dangerous pathogens, to modern versions, such as electromagnetic radiation and other directed energy weapons.").

[76] Minnow, *supra* note 33 ("Yet, this approach would better describe 'identities' than analogies; that is, circumstances that actually are identical. Where analogy makes a contribution is where the disputed instance actually differs in some noticeable and worrisome way from the comparison point. Recent work in cognitive theory suggests that analogical reasoning is an instance of problem-solving methods that match patterns in the environment with stored schemas for solutions or solution procedures").

[77] Espionage is generally thought of as a domestic rather than international law problem. However, one could argue that it may violate the non-intervention principle. Regardless, though it warrants categorization herein, it is generally tolerated by states. Everyone does it, and everyone wants to keep doing it; if a person gets caught, it will be handled domestically rather than internationally.

[78] Merriam-Webster Dictionary, https://www.merriam-webster.com/dictionary/espionage (last visited Mar. 29, 2019).

[79] Rid, *supra* note 56, 20.

[80] Christopher Mewett, *Understanding War's Enduring Nature Alongside its Changing Character*, War on the Rocks (Jan. 21, 2014), https://warontherocks.com/2014/01/understanding-wars-enduring-nature-alongside-its-changing-character/ (last visited Mar. 25, 2019) (hereinafter Mewett, *Understanding War)* ("The *character* of war describes the changing way that war as a phenomenon manifests in the real world." (emphasis in original)).

[81] A machine is a "device or apparatus consisting of fixed and moving parts that work together to perform some function." Computers, system and network components, and the objects which are controlled through them meets this definition. Given that a cyberspace operation cannot target an object unless it is "wired" in some form, it is appropriate to use a term like "machine" when speaking of cyberspace operations because it is both broadly inclusive within that context and simultaneously exclusive in that it distinguishes between the capabilities of a bomb, for instance, and a mode of operation that requires a network. For the definition of "machine" quoted above, *see* Black's Law Dictionary (Brian Garner ed., 8th ed., 2004).

[82] Tatum, *supra* note 44, 37.

[83] *Id*.

[84] *See Id*. at fig, 9, 40.

[85] *See, e.g*., Kim Zetter, *A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever*, Wired (Jan. 8, 2015, 5:30 AM), https://www.wired.com/2015/01/german-steel-mill-hack-destruction/ (last visited Jan. 4, 2019) (A cyberspace operation disrupted the control of a blast furnace and prevented it from being shut down, thereby causing the furnace to remain hot and cause "massive" damage. Presumably, this means the functionality of the machine was damaged).

[86] Beard, *supra* note 24, 99 ("Complex combinations of factors that are said to inform a consequentialist approach to the *jus ad bellum* in cyberspace thus belie a simpler truth (and dilemma): legitimate cyber attacks must closely resemble not only the effects but also the *acts* that make up conventional armed attacks (involving physical armed force).").

[87] There is no resemblance, for instance, between electronic warfare and biological weapons, another form of non-kinetic armed force.

[88] Beard, *supra* note 24, 98.

[89] *Id*. at 99.

[90] Minnow, *supra* note at 33 (emphasis added).

[91] Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 Yale J. Int'l L. 421, 427-428 (2011); *see also*, Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 Colum. J. Transnat'l L. 885, 904 (1999).

[92] Treaty interpretation, like many other areas of the law, has principles that guide the efforts of the interpreters. The first such principle is the requirement to give treaty terms their ordinary meaning in light of the treaty's object and purpose. Vienna Convention on the Law of Treaties, art. 31, May 23, 1969, 1155 U.N.T.S. 331 (hereinafter Vienna Convention). To meet this requirement, a treaty must be interpreted within the context in which it was written, a concept which includes the treaty's main body, its preamble, and subsequent action of states that relate to the treaty. Examining these components does not, however, always lead to a clear answer. To resolve ambiguities, or to reinforce a non-ambiguous interpretation, it is permissible to consider the circumstances surrounding the treaty's conclusion and the record of its drafting. A search for what Article 2(4) means by "force" must therefore include an examination of the UN Charter's preamble, main body, and any subsequent state actions interpreting it. Vienna Convention, art. 32.

[93] U.N. Charter, Preamble.

[94] *Id*. (emphasis added).

[95] *Id*. at art. 1(1).

[96] *Id*. at art. 2(3).

[97] *Id*. at art. 2(4).

[98] *Id.* at art. 44; *see also*, Schmitt, *supra* note 91, 904 ("The wording of Article 44 further supports a restrictive interpretation. It states, 'When the Security Council has decided to use force it shall, before calling upon a Member not represented to provide armed forces ….' 'Force' appears, as in Article 2(4), without the qualifier 'armed,' but, as demonstrated by the reference to "armed forces,' clearly contemplates that the force used be armed.").

[99] Schmitt, *supra* note 91, 904 ("the Preamble includes among Charter purposes the goal that 'armed force … not be used save in the common interest ….' If the Article 2(4) prohibition were intended to extend beyond armed force, then presumably the preamble, for reasons of internal consistency, would not have included the term 'armed.' After all, the Charter's articles are designed to effectuate its preambular aspirations. Thus, preambular terminology is logically interpreted more broadly than that contained in the articles.").

[100] When interpreting treaties, it is permissible to go beyond the immediate text to consider, "any subsequent agreement between the parties regarding the interpretation of the treaty or the application of its provisions" and "any subsequent practice in the application of the treaty which establishes the agreement of the parties regarding its interpretation." Vienna Convention, art. 31.

[101] U.N. G.A. Res. 3314 (XXIX), Definition of Aggression (Dec. 14, 1974) (hereinafter UNGAR 3314).

[102] Vienna Convention, art. 32.

[103] The exceptionally bloody Battle of Okinawa concluded only a week before the UN Charter was signed. Robert Gandt, The Twilight Warriors 338 (2010). And, had the power of atomic weapons not intervened, the invasion of the Japanese home islands would have occurred in November 1945, well after the UN Charter entered into force. *See* Walter R. Borneman, The Admirals: Nimitz, Halsey, Leahy, and King – The Five Star Admirals Who Won the War at Sea 444 (2012).

[104] U.N. Charter, art. 39, 51.

[105] *Cyber Strategy & Policy: International Law Dimensions, Hearing Before the S. Armed Serv. Comm.,* 115th Cong. 1, 2 (2017) (statement of Matthew C. Waxman, Professor of Law, Columbia Law School) (hereinafter Waxman Statement) ("A more legally precise way to frame the 'act of war' question, then, is whether a cyber-attack could violate the UN Charter's prohibitions of force or could amount to an armed attack.").

[106] Schmitt, *supra* note 91, 905.

[107] *Id.*

[108] Citing a 1998 United Nations International Children's Emergency Fund (UNICEF) survey, the International Committee of the Red Cross reported in 1999 that after nearly a decade of economic sanctions by the international community, the mortality rate of Iraqi children under the age of five had more than doubled since the previous decade. *Iraq: 1989-1999, A Decade of Sanctions*, Int'l Comm. Of the Red Cross Report (Dec. 14, 1999), https://www.icrc.org/en/doc/resources/documents/report/57jqap.htm (last visited Aug. 4, 2021) (citing Iraq Surveys Show 'Humanitarian Emergency,' UNICEF Information Newsline (Aug. 12, 1999), https://www.unicef.org/newsline/99pr29.htm [since being cited, this link appears to no longer be available]). A 1995 New York Times article placed the death toll at 576,000 children, and also detailed widespread malnourishment and stunted development amongst Iraqi children that managed to survive. See Barbara Crossette, Iraq Sanctions Kill Children, U.N. Reports, The New York Times (Dec. 1, 1995), https://www.nytimes.com/1995/12/01/world/iraq-sanctions-kill-children-un-reports.html (last visited Mar. 29, 2019).

[109] T.F. Schmidt, *The 1964 Presidential Race: Election Operation in Chile*, 43-48, Central Intelligence Agency Online Reading Room, https://www.cia.gov/library/reading-room/docs/DOC_0006122559.pdf (last visited Mar. 29, 2019).

[110] Louis Nelson, *Cardin: Russia's Election Meddling is 'An Act of War,'* Politico (Nov. 1, 2017, 11:03 AM), https://www.politico.com/story/2017/11/01/russia-meddling-us-elections-ndi-event-244414 (last visited Dec 31, 2018).

[111] Ellen Nakashima, *Russia's Apparent Meddling in U.S. Election is Not an Act of War, Cyber Expert Says*, Washington Post (Feb. 7, 2017), https://www.washingtonpost.com/news/checkpoint/wp/2017/02/07/russias-apparent-meddling-in-u-s-election-is-not-an-act-of-war-cyber-expert-says/ (last visited March 27, 2019).

[112] After all, "attempts by states … to promote their views and influence the actions of other states … are common and even a fundamental part of international relations *See* Beard, *supra* note 24, 135.

[113] U.N. Charter, art. 1(1).

[114] Tobias Kliem, *You Can't Cyber in Here, This is the War Room! A Rejection of the Effects Doctrine on Cyberwar and the Use of Force in International Law*, Journal on the Use of Force and Int'l. Law 344, 349 (2017) (hereinafter Kliem, *War Room*).

[115] Waxman Statement, *supra* note 105 ("A more legally precise way to frame the 'act of war' question, then, is whether a cyber-attack could violate the UN Charter's prohibitions of force or could amount to an armed attack.").

[116] *See* U.N. Charter, Preamble.

[117] *Id.* at art. 2(1).

[118] *Id*. at art 2(3).

[119] Schmitt, *supra* note 91, 906 (discussing the exclusion of economic coercion from Article 2(4)'s prohibition on the threat or use of force).

[120] U.N. Charter, art. 51.

[121] Statute of the International Court of Justice, art. 38, ¶ 1(d).

[122] *See, Id*. at ¶ 20.

[123] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Merits, Judgment, 1986 I.C.J. Rep. 14, ¶ 228 (June 27) (hereinafter *Nicaragua v. U.S.*). The ICJ's decision interprets the customary international law version of the prohibition against the threat or use of force, and while Article 2(4) and its corollary in customary international law are not necessarily identical, the two standards are substantially similar and thus a judgement on one is tantamount to a judgement on the other. S*ee Nicaragua v. U.S.*, ¶¶ 174-188, 292(4). Additionally, UN General Assembly Resolution 3314, passed in 1974, declared that sending a group to carry out acts of armed force against another state is an "act of aggression." The definition of "act of aggression" in the resolution very closely mirrors the text of Article 2(4), which suggests that acts of aggression and uses of force are the same in concept if not in gravity. The importance of Resolution 3314 is that it is essentially state commentary on the text of the UN Charter. It thus follows that one state sending someone else to use force on its behalf, in addition to a violation of customary international law, is also a violation of Article 2(4). *See* UNGAR 3314, *supra* note 101 ("acts of aggression" are "use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with" the purpose of the UN Charter.). *See also*, Todd C. Huntley, *Controlling the Use of Force in Cyberspace: The Application of the Law of Armed Conflict During a Time of Fundamental Change in the Nature of Warfare*, 60 Naval L. Rev. 1, 16 (2010).

[124] *Nicaragua v. U.S.*, ¶ 228.

[125] *Id.* at ¶ 20.

[126] *Id*. at ¶ 269.

[127] *Id*. at ¶ 228; *see also*, G.A. Res. 2625 (XXV), Declaration on Principles of International Law Concerning Friendly Relations and Co-operation Among States in Accordance with the Charter of the United Nations, (Oct. 24, 1970).

[128] *Nicaragua v. U.S.*, ¶ 228.

[129] Resolution 2625 is a state-generated document based on the terms of the UN Charter. Thus, Resolution 2625 is not just a majority vote on a particular subject, but arguably a "subsequent agreement between the parties [to a treaty] regarding the interpretation of the treaty or the application of its provisions." Vienna Convention, art. 31. Thus, the ICJ's interpretation is not just a judicial interpretation, but an application of state practice used to interpret the UN Charter.

[130] The idea that the *Nicaragua* decision threw open the door to what may be considered a use of force is a foundational tenet of the effects model. As demonstrated above, however, the concept of force is not so open as the effects model presumes, which undermines the entire basis for its analogy. Schmitt, *supra* note 91, 913-914 ("In that computer network attack cuts across the instrument-based distinction employed as prescriptive short-hand, it becomes necessary to shift cognitive approach if one wishes to continue to operate within the existing framework …. Yet, the holding of the ICJ in the Nicaragua Case with regard to arming and training the contras suggested that other forms of "force" were not necessarily excluded. Therefore, the use of force line must lie somewhere between economic coercion and the use of armed force. The question becomes how to locate the point of demarcation, at least with regard to this new genre of coercion.").

[131] When interpreting treaties, it is permissible to go beyond the immediate text to consider, "any subsequent agreement between the parties regarding the interpretation of the treaty or the application of its provisions" and "any subsequent practice in the application of the treaty which establishes the agreement of the parties regarding its interpretation." Vienna Convention, art. 31.

[132] *See generally*, Michael Schmitt & Liis Vihul, *International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms*, Just Security (Jun. 30, 2017), https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/ (last visited Mar. 25, 2019).

[133] Beard, *supra* note 24, 99 ("Complex combinations of factors that are said to inform a consequentialist approach to the *jus ad bellum* in cyberspace thus belie a simpler truth (and dilemma): legitimate cyber attacks must closely resemble not only the effects but also the *acts* that make up conventional armed attacks (involving physical armed force).").

[134] Vienna Convention, art. 31.

[135] Statute of the International Court of Justice, art. 59.

[136] Rosa Brooks, How Everything Became War and the Military Became Everything: Tales from the Pentagon 218 (2016).

[137] Tallinn 1.0 observes that "no international cyber incidents have, as of 2012, been unambiguously and publically characterized by the international community as … an armed attack." See Tallinn 1.0, *supra* note 4, 57. Notably, the international community also has not unambiguously characterized a cyber-incident as a use of force, which to many states is a lower threshold than armed attack.

[138] Joshua Davis, *Hackers Take Down the Most Wired Country in Europe,* Wired, (Aug. 21, 2007, 12:00 PM), https://www.wired.com/2007/08/ff-estonia/ (last visited Mar. 3, 2020).

[139] *See* U.S. Dept. of Homeland Security CISA, *Understanding Denial-of-Service Attacks*, Security Tip (ST04-015) (Nov. 20, 2019), https://www.us-cert.gov/ncas/tips/ST04-015 (last visited Mar. 8, 2020).

[140] Davis, *supra* note 138.

[141] *Id.*

[142] Davis, *supra* note 138; *see also*, Rain Ottis, *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective,* Cooperative Cyber Defense Centre of Excellence, https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf (last visited Mar. 3, 2020).

[143] Ottis, *supra* note 142, 1; *see also*, Davis, *supra* note 138.

[144] Soviet soldiers liberated Tallinn from German control during World War II. For their part, Estonians viewed the statue as a symbol of Soviet oppression following the country's "liberation." Ottis, *supra* note 142, 1.

[145] Ottis, *supra* note 142, 2.

[146] *Id.*

[147] These remarks were made during a celebration on May 9, 2007 commemorating the allied victory over Nazi Germany. Davis, *supra* note 138.

[148] *See generally*, Ottis, *supra* note 142.

[149] North Atlantic Treaty, art. 5, Apr. 4, 1949, 63 Stat. 2241, 34 U.N.T.S. 243.

[150] Ian Traynor, *Russia Accused of Unleashing Cyberwar to Disable Estonia*, The Guardian (May 16, 2007, 9:32 PM), https://www.theguardian.com/world/2007/may/17/topstories3.russia (last visited Mar. 8, 2020) (quoting Jaak Aaviksoo, the Estonian minister of defense at the time of the attack).

[151] *See* Ottis, *supra* note 142.

[152] The United States for one has affirmatively stated that a severe enough cyber-attack might be considered a use of force and an armed attack. *See supra* note 3.

[153] *See* Press Release, U.S. Dept. of Justice, *Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector*, (Mar. 24, 2016), https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged (last visited Mar. 13, 2020) (hereinafter, Seven Iranians Press Release); *see also*, Dustin Volz & Jim Finkle, *U.S. Indicts Iranians for Hacking Dozens of Banks, New York Dam*, Reuters (Mar. 24, 2016), https://www.reuters.com/article/us-usa-iran-cyber/u-s-indicts-iranians-for-hacking-dozens-of-banks-new-york-dam-idUSKCN0WQ1JF (last visited Mar. 19, 2020).

[154] *Seven Iranians Press Release*, *supra* note 153.

[155] Electromagnetic interference is "any electromagnetic disturbance … that interrupts, obstructs, or otherwise degrades or limits the effective performance of electronics and electrical equipment." Electromagnetic jamming is the "deliberate radiation, reradiation, or reflection of electromagnetic energy for the purpose of preventing or reducing an enemy's effective use of the electromagnetic spectrum …." *DoD Dictionary*, *supra* note 38, 70.

[156] Antonio J. Mendez & Jonna Mendez, The Moscow Rules: The Secret CIA Tactics that Helped America Win the Cold War 13 (2019) (describing the Soviet use of microwaves to collect intelligence and jam communications at the United States embassy in Moscow); *see also*, Ryan Browne, *Russia Jammed GPS During Major NATO Military Exercise with US Troops*, CNN (Nov. 14, 2018, 11:48 AM), https://www.cnn.com/2018/11/14/politics/russia-nato-jamming/index.html (last visited Mar. 19. 2020).

[157] Characterizing the Estonian attack as jamming is somewhat controversial, as some experts maintain that the attack's interruption of commercial activities places the attack in a different category. Tallinn 1.0, *supra* note 4, 197. This position seems to presume that information is somehow more valuable when used in a transactional function. However, information has always been and will continue to be valuable outside of commercial transactions—sometimes extremely so—to governments, businesses, private citizens, and so on. Furthermore, there seems little reason to consider a contract negotiation foiled by a DDoS attack as substantially different from telephone-based negotiation foiled by electronic warfare. It is also noteworthy that the UN Security Council has several non-armed force options that it may use to give effect to its decisions. Included in these measures is the "complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, and other means of communication …." Such disruption of communications is remarkably similar to what was accomplished by the DDoS attack against Estonia. U.N. Charter, art. 41.

[158] The politically coercive impact is difficult to measure, but it can be safely asserted that Estonians are aware that their internal affairs are not beyond the influence of the Russian state even in a post-Soviet world.

[159] *See*, *e.g.*, Elizabeth Gurdus, *We're Headed for 'Cyber Pearl Harbor,' Says Adm James Stavridis*, CNBC (Dec. 15, 2016, 10:37 AM), https://www.cnbc.com/2016/12/15/were-headed-at-a-cyber-pearl-harbor-says-adm-james-stavridis.html (last visited Jan. 11, 2019); Elisabeth Bumiller & Thomas Shanker, *Panetta Warns of Dire Threat of Cyberattack on U.S.*, The New York Times (Oct. 11, 2012), https://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html (last visited Jan. 11, 2019); and Natasha Turak, *The Next 9/11 Will be a Cyberattack, Security Expert Warns*, CNBC, (June 1, 2018), https://www.cnbc.com/2018/06/01/the-next-911-will-be-a-cyberattack-security-expert-warns.html (last visited Mar. 14, 2019). For a more measured discussion, *see*, Troy Amerding, *'Cyber Pearl Harbor' Unlikely, But Critical*

Infrastructure Needs Major Upgrade, Forbes (Oct. 23, 2018, 1:02 AM), https://www.forbes.com/sites/taylorarmerding/2018/10/23/cyber-pearl-harbor-unlikely-but-critical-infrastructure-needs-major-upgrade/?sh=6a943c67f8b6 (last visited Jan. 11, 2019).

[160] Rid, *supra* note 56, 18.

[161] Rid, *supra* note 56, 19.

[162] Rid, *supra* note 56, 19.

[163] Rid, *supra* note 56, 7.

[164] Kim Zetter, *An Unprecedented Look at Stuxnet, The World's First Digital Weapon*, Wired, (Nov. 3, 2014, 6:30 AM), https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/ (last visited Mar. 15, 2019) (hereinafter Zetter, *Unprecedented Look*).

[165] William J. Broad, John Markoff, & David E. Sanger, *Israeli Test on Worm Called Crucial in Iran Nuclear Delay,* The New York Times, (Jan. 15, 2011), https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html (last visited Mar. 9, 2019).

[166] Associated Press, *Iran Blames U.S., Israel for Stuxnet Computer Worm* (Apr. 16, 2011, u/d Dec. 12, 2015), https://www.foxnews.com/tech/iran-blames-u-s-israel-for-stuxnet-computer-worm (last visited Mar. 9, 2019).

[167] David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, The New York Times (June 1, 2012), https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html (last visited Mar. 9, 2019).

[168] U.N. Charter, art. 39.

[169] Aerial Incident of 3 July 1988 (Iran v. U.S.), Application, 1989 I.C.J. 79 (May 1989); Oil Platforms (Iran v. U.S.), Application, 1992 I.C.J. 90 (Nov. 1992); Certain Iranian Assets (Iran v. U.S.), Application, 2016 I.C.J. 164 (June 2016); and Alleged violations of the 1955 Treaty of Amity, Economic Relations, and Consular Rights (Iran v. U.S.), Order 2018 I.C.J. 175 (Oct. 2018).

[170] Fredrik Dahl, *Q&A: Is there a 'Right' to Enrich Uranium? Iran Says Yes, U.S. No*, Reuters (Nov. 23, 2013, 1:49 AM), https://www.reuters.com/article/us-iran-nuclear-rights-idUSBRE9AL0R120131123 (last visited Mar. 15, 2019); *see also*, Treaty on the Non-Proliferation of Nuclear Weapons, art. 4, Jul. 1, 1968, 21 UST 483, 729 UNTS 161.

[171] Iran called itself the "target of sabotage," which notably is not "use of force" or "act of aggression." Following a state action of this type, the exact phrasing matters a great deal. *See* Beard, *supra* note 24, 137 (quoting, Thomas Erdbrink, *Ahmadinejad: Iran's Nuclear Program Hit by Sabotage,* Wash. Post (Nov. 29, 2010, 2:23 PM}, https://www.washingtonpost.com/wp-dyn/content/article/2010/11/29/AR2010112903468.html).

[172] The prevailing opinion of western legal scholars runs unambiguously in the other direction. *See* Tallinn 1.0, *supra* note 4, 45 ("The clearest cases are those cyber operations, such as the employment of the Stuxnet worm, that amount to a use of force.").

[173] "Air gap" is a term used to describe closed networks, which is to say networks that are unconnected to the outside world. To get Stuxnet onto an air-gapped network, someone—perhaps wittingly, perhaps not—had to put the code onto the closed network from within the facility. *See* Rid, *supra* note 56, 18.

[174] *See* Kliem, *supra* note 114, 363.

[175] Beard, *supra* note 24, 134.

[176] *See*, *e.g.,* FM 3-12, *supra* note 45, 1-26 (lasers, radio frequency weapons, directed microwaves, and particle beams).

[177] Wilson, *supra* note 48, 6.

[178] Gary Corn & Eric Jensen, *The Technicolor Zone of Cyberspace – Part I: Analyzing the Major U.K. Speech on International Law of Cyber*, Just Security (May 30, 2018), https://www.justsecurity.org/57217/technicolor-zone-cyberspace-part/ (last visited Mar. 12, 2020) ("Further, the prevailing view is that most, if not all, documented cyber action taken by states to date have fallen below the 'use of force' threshold.").

[179] The GGE agreed in 2013 that international law, and in particular the UN Charter, applies to cyberspace operations; *see* Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, U.N. Doc. A/68/98* (2013). Regarding more specific laws of war, the GGE has gone only as far as to "note" the existence of International Humanitarian Law principles like, "where applicable, the principles of humanity, necessity, proportionality and distinction." Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, U.N. Doc. A/70/174, ¶ 28(d) (2015). For a summation of the GGE's years of work, *see generally*, Schmitt & Vihul, *supra* note 132.

[180] Michael Connell & Sarah Vogler, *Russia's Approach to Cyber Warfare*, CNA Analysis & Solutions (Mar. 2017), https://www.cna.org/cna_files/pdf/DOP-2016-U-014231-1Rev.pdf (last visited Mar. 27, 2019). (quoting *The Military Doctrine of the Russian Federation*, approved by Russian Federation presidential edict on February 5, 2010 (translated). ("According to the Military Doctrine of the Russian Federation (2010), one of the features of modern military conflicts is "*the prior implementation of measures of information warfare* in order to achieve political objectives without the utilization of military force and, subsequently, in the interest of shaping a favourable response from the world community to the utilization of military force.").

[181] Li Zhang, *A Chinese Perspective on Cyber War*, 94 Int'l Rev. of the Red Cross 801 (2012) ("[T]here is only one fundamental goal: namely, to avoid the use of force or threat of force to the greatest extent possible and to prevent the outbreak of cyber warfare. The threshold for lawful use of force in the cyber domain should be high ….").
See also, Ashley Deeks, *Tallinn 2.0 and a Chinese View on the Tallinn Process*, Lawfare (May 31, 2015, 2:00 PM), https://www.lawfareblog.com/tallinn-20-and-chinese-view-tallinn-process (last visited Mar. 25, 2019); and *see generally*, Kimberly Hsu & Craig Murray, *China and International Law in Cyberspace*, U.S.-China Economic and Security Review Commission Staff Report, May 6, 2014, https://www.uscc.gov/sites/default/files/Research/China%20International%20Law%20in%20Cyberspace.pdf (last visited Dec. 19, 2018).

[182] Since at least 2011, the United States has held that a severe enough cyberspace attack could result in its invocation of Article 51's right of self-defense. Notably, self-defense is not limited to responding in cyberspace; the United States could conceivably respond to a cyberspace attack with conventional kinetic force. *See International Strategy for Cyberspace* (May 2011), *supra* note 3.

[183] *National Cyber Strategy of the United States of America* (Sept. 2018), *supra* note 3, 2-3; *see also*, The White House, *National Security Strategy of the United States of America*, 28 (Dec. 2017).

[184] David A. Koplow, ASAT-isfaction: Customary International Law and the Regulation of Anti-Satellite Weapons, 30 Mich. J. Int'l L. 1187, 1225 (2008-2009) ("To evaluate the relevant behavior of States, CIL contemplates the full range of a country's words as well as deeds, silences as well as inactions, and oral as well as written statements."). Professor Koplow's article was an examination of customary international law rather than a treaty like the UN Charter; however, state practice gives meaning to treaty terms in the same way it gives meaning to the boundaries of customary international law. Further, there is also a rule of customary international law prohibiting the threat or use of force, to which Professor's Koplow's statement is even more directly applicable.

[185] Minnow, *supra* note 33.

[186] To the extent cyberspace operations resemble old-fashioned political or economic coercion, espionage, or even domestic criminal activity, that is how those operations should be categorized. Beard, *supra* note 24, 128 ("The very nature of a hostile cyber act against an economic target makes it far more likely that the act will constitute an economic, property, or security crime under a state's domestic law than an act of violence governed by the IHL regime or an armed attack for purposes of the *jus ad bellum.* Hostile, state-sponsored cyber acts against economic targets may in fact be indistinguishable from increasingly common acts of cyber fraud, larceny, or espionage."); *see also*, Charles J. Dunlap Jr., *Perspectives for Cyber Strategists on Law for Cyberwarfare*, Strategic Studies Quarterly, Mar. 1, 2011, at 81, 84 ("All things being equal, cyber strategists should default to the law enforcement modality. This makes practical sense, because many experts see cyber crime (as opposed to cyberwar) as the most serious and most common threat in the cyber domain. 'Crime,' incidentally, could include acts at the behest of a nation-state, such as cyber espionage targeting a government or industry.")

[187] *See* Hague (II) 1907, *supra* note 11.

[188] Schmitt, *supra* note 91, 905. Referring to most cyberspace operations, even very damaging ones, as uses of force is arguably a return to the bad old days that failed to prevent World War II.

[189] Mewett, *supra* note 80 ("War's nature is violent, interactive, and fundamentally political."); *see also*, Corn & Jensen, *supra* note 178 ("Whether and how to hold states like Russia accountable for such actions is ultimately a political question"—referencing Russian hacking of United States critical infrastructure and poisoning a former Russian operative and his daughter in the United Kingdom).

[190] *See, generally, supra* note 159.

[191] Schmitt, *supra* note 91, 916.

[192] Hathaway & Crootof, *supra* note 23, 823 (citing Barton Gellman, *Cyber Attacks by al Qaeda Feared; Terrorists at Threshold of Using Internet as Tool of Bloodshed, Experts Say*, Wash. Post, Jun. 27, 2002, at A1.).

[193] Lotrionte, *supra* note 14, 82.

[194] In 2015, an intrusion in the systems of the United States Office of Personnel Management yielded security clearance data on more than four million federal employees. The intrusion was attributed to the Chinese government. Brendan I. Koerner, *Inside the Cyberattack That Shocked the US Government*, Wired (Oct. 23, 2016, 5:00 PM), https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/ (last visited Mar. 14, 2019).

[195] "Moonlight Maze" was a series of network intrusions on United States Government networks that resulted in the theft of sensitive information and gathering of data relevant to military operations. Rid, *supra* note 56, 15; *see also*, Lolita C. Baldor, *US Prepared to Strike Back Against Cyberattacks Amid Report of Naval Systems Breaches*, Associated Press (Mar. 13, 2019), https://www.militarytimes.com/news/pentagon-congress/2019/03/14/us-prepared-to-strike-back-against-cyberattacks-amid-report-of-naval-systems-breaches/ (last visited Mar. 16, 2019).

[196] Nelson, *supra* note 110.

[197] *See generally*, Rid, *supra* note 56.

[198] Libicki, *supra* note 65, 89.

[199] *Id.*

[200] Attribution of cyberspace operations may be limited to determining which states had the means of undertaking such an operation, and who also had a motive to do so and an opportunity. Libicki, *supra* note 65, 90-91.

[201] Robert Bebber, *Winning the Phase 0 War*, Foreign Policy (Jan. 7, 2016, 10:23 AM), https://foreignpolicy.com/2016/01/07/winning-the-phase-0-war/ (last visited Dec. 19, 2019); *see also*, Baldor, *supra* note 195.

[202] Baldor, *supra* note 195.

[203] *See*, *supra* note 3. This is particularly true when the potential adversary has overwhelmingly powerful conventional forces like those of the United States. Sidney J. Freeberg Jr., *Russia, China are Outmaneuvering US: Generals Recommend New Authorities, Doctrine*, Breaking Defense (Jun. 15, 2018, 3:29 PM), https://breakingdefense.com/2018/06/russia-china-are-outmaneuvering-us-generals-recommend-new-authorities-doctrine/ (last visited Dec. 19, 2018)

[204] Samantha Raphelson, *Report: Russian Hackers Had the Ability to Shut Down U.S. Power Plants*, NPR (Mar. 16, 2018, 5:02 PM), https://www.npr.org/2018/03/16/594371939/u-s-accusesrussia-of-cyberattacks-on-energy-infrastructure (last visited Mar. 20, 2020).

[205] Harold Hongju Koh, Legal Advisor, Dept. of State, Address at the U.S. Cyber Command Inter-Agency Legal Conference: International Law in Cyberspace (Sep. 18, 2012), https://2009-2017.state.gov/s/l/releases/remarks/197924.htm (last visited Mar. 16, 2020). The United Kingdom has provided signaling similar to that of the United States. *See* Jeremy Wright, Atty. Gen., United Kingdom, Address at the Chatham House Royal Institute for International Affairs: Cyber and International Law in the 21st Century (May 23, 2018), https://www.chathamhouse.org/event/cyber-and-international-law-21st-century (last visited Mar. 16, 2020).

[206] *See* Prableen Bajpai, *The 5 Largest Economies in the World and Their Growth in 2020*, Nasdaq (Jan. 22, 2020, 2:24 PM), https://www.nasdaq.com/articles/the-5-largest-economies-in-the-world-and-their-growth-in-2020-2020-01-22 (last visited Mar. 19, 2020) (noting that the United States has the largest economy in the world and currently comprises one-fourth of the world economy).

[207] This is not to say that a sophisticated terrorist network or criminals would refrain from doing something of this nature. However, in the world of inter-state relations to which the UN Charter applies, such an attack would be mutually destructive and thus a rather poor idea.

[208] Michael N. Schmitt, *Cyber Operations and the Jud Ad Bellum Revisited*, 56 Vill. L. Rev. 569, 573 (2011). ("It would be no less absurd to suggest that cyber operations that generate consequences analogous to those caused by kinetic force lie beyond the prohibition's reach, than to exclude other destructive non-kinetic actions, such as biological or radiological warfare. Accordingly, cyber operations that directly result (or are likely to result) in physical harm to individuals or tangible objects equate to armed force, and are therefore uses of force.").

[209] K Ganesan, et al., Chemical Warfare Agents, J. Pharm Bioall Sci, Aug. 16, 2010, at 166, http://www.jpbsonline.org/article.asp?issn=09757406;year=2010;volume=2;issue=3;spage=166;epage=178;aulast=Ganesan (last visited Mar. 27, 2019).

[210] Mark Perry, *Why the World Banned Chemical Weapons*, Politico (Apr. 16, 2017, 6:30 AM), https://www.politico.eu/article/why-the-world-banned-chemical-weapons/ (last visited Jan. 3, 2019).

[211] Rid, *supra* note 56, 17-20.

[212] Rid, *supra* note 56, 18.

[213] David Stout, *Coast Guard Using Sharpshooters to Stop Boats*, The New York Times (Sep. 14, 1999), https://www.nytimes.com/1999/09/14/us/coast-guard-using-sharp-shooters-to-stop-boats.html (last visited Mar. 17, 2019).

[214] Tatum, *supra* note 44, 37.

[215] Zetter, *supra* note 164.

[216] *See* TALLINN 1.0, *supra* note 4, 45. (The only disagreement seems to be on whether it was also an armed attack). *See also*, TALLINN 1.0, *supra* note 4, 58 ("A closer case is the 2010 Stuxnet operations. In light of the damage they caused to Iranian centrifuges, some members of the International Group of Experts were of the view that the operations had reached the armed attack threshold ….").

[217] Gary Brown & Keira Poellet, *The Customary International Law of Cyberspace*, Strategic Studies Quarterly, Sep. 03, 2012, 132.

[218] Kliem, *supra* note 114, 365.

[219] *See generally*, Schmitt, *supra* note 91.

[220] Schmitt, *supra* note 91, 913-914 ("In that computer network attack cuts across the instrument-based distinction employed as prescriptive short-hand [force], it becomes necessary to shift cognitive approach if one wishes to continue to operate within the existing framework.").

[221] Schmitt, *supra* note 91, 913-914 ("Yet, the holding of the ICJ in the Nicaragua Case with regard to arming and training the contras suggested that other forms of 'force' were not necessarily excluded. Therefore, the use of force line must lie somewhere between economic coercion and the use of armed force.").

[222] Focusing on negative consequences alone would likely, for instance, capture behavior more akin to economic or political coercion or espionage, none of which are uses of force. Schmitt, *supra* note 91, 917 ("… simply ask to what degree the consequences of computer network attack threaten shared community values …. The flaw in doing so lies in the fact that it calls for a new normative architecture altogether to handle such actions, an architecture that amounts to more than an interpretive dilation of the use of force standard. It would constitute a new standard.").

[223] Widening the aperture of the effects model is often suggested, as its critics most often find it under rather than over inclusive. *See*, *e.g.,* Waxman, *supra* note 91, 436 ("A significant problem with this view is that in a world of heavy economic, political, military, and social dependence on information systems, the 'nonviolent' harms of cyber-attacks could easily dwarf the 'violent' ones. Consider, for example, a take-down of banking systems, causing cascades of financial panic, or the disabling of a power grid system for an extended period, causing massive economic disruption and public health emergencies."); *see also*, Lotriont*e*, *supra* note 14, 82 (" For those cyber operations that are disruptive, interrupting the functionality of a target, but failing to cause lasting physical damage, a strict effects-based equivalence test under the law raises questions as to whether such attacks would constitute a 'use of force' under article 2(4). Such a narrow approach based on kinetic effects fails to take into account the dependency of modern society on the functioning of computer networks.").

[224] Schmitt*, supra* note 91, 917.

[225] Schmitt*, supra* note 91, 914 ("Economic and political coercion can be delimited from the use of armed force by reference to various criteria. The following number among the most determinative: [s]everity … [i]mmediacy … [d]irectness … [i]nvasiveness … [m]easurability … [and] presumptive legitimacy."); *see also*, TALLINN 1.0, *supra* note 4, 48-51 (adding "state involvement" and "military character" as additional criteria.).

[226] TALLINN 1.0, *supra* note 4, 48.

[227] Hathaway & Crootof, *supra* note 23, 847-848 ("These factors are illuminating, but they call for such a wide-ranging inquiry that they may not provide sufficient guidance to decision makers. In other words, different analysts applying this version of the effects-based approach might plausibly classify all or none of the examples listed above as armed attacks.").

[228] Tallinn 1.0, *supra* note 4, 216-218.

[229] The total cost of the DDoS attack to Estonia is difficult to quantify, but one Estonian bank admitted its losses were approximately $1 million. The total cost to the Estonian economy and to its government was undoubtedly much higher. *See* Valentinas Mite, *Estonia: Attacks Seen as First Case of 'Cyberwar*,' Radio Free Europe Radio Liberty (May 30, 2007), https://www.rferl.org/a/1076805.html (last visited Mar. 18, 2020).

[230] *See*, *e.g.,* Waxman, *Back to the Future*, *supra* note 91, 436; *see also*, Lotrionte, *supra* note 14, 82.

[231] Beard, *supra* note 24, 117 ("… diminish restrictions on the use of force, thereby significantly weakening key safeguards upon which the international community relies ….").

[232] Schmitt, *supra* note 91, 913 ("One narrow category of computer network attack is easily dealt with. CNA specifically intended to directly cause physical damage to tangible property or injury or death to human beings is reasonably characterized as a use of armed force and, therefore, encompassed in the prohibition.").

[233] Kliem, *supra* note 14, 353.

[234] Tallinn 1.0, *supra* note 4, 48 ("Accordingly, whatever 'force' may be, it is not mere economic or political coercion. Cyber operations that involve, or are otherwise analogous to, these coercive activities are definitely not prohibited uses of force.").

[235] Kliem, *supra* note 114, 353; *see also*, Tallinn 2.0, *supra* note 4, 331.

[236] Tallinn 2.0, *supra* note 4, 331.

[237] Tallinn 1.0, *supra* note 4, 46.

[238] Some have argued for a more "elastic" *jus ad bellum* in which large scale economic harm may be sufficient to violate Article 2(4). *See*, Michael N. Schmitt, *Cyberspace and International Law: The Penumbral Mist of Uncertainty*, 126 Harv. L. Rev. F. 176, 178 (2013) ("The *jus ad bellum* is likewise characterized by interpretive elasticity. 'Use of force' irrefutably includes acts that cause physical damage or injury, but not traditional economic or political sanctions. However, no authoritative criteria exist to qualify acts falling in the twilight between physically harmful cyberoperations and those that are purely economic or political in nature …. Moreover, it is questionable whether the historic exclusion of economic warfare should be interpreted as extending to cyberoperations that generate dramatic economic consequences.").

[239] Beard, *supra* note 24, 132.

[240] Beard, *supra* note 24, 117.

[241] Minnow, *supra* note 33.

[242] Hollis, *supra* note 25, 1023-1061.

Surfing On Base

*Major Edwin C. Kisiel III**

* Major Edwin C. Kisiel III, USAF, (LL.M., Environmental Law, George Washington University Law School, with highest honors (2019); J.D., Liberty University School of Law, *magna cum laude* (2011); B.S., Government, Liberty University, *summa cum laude* (2008)) is the Deputy Staff Judge Advocate for 28th Bomb Wing, Ellsworth Air Force Base, South Dakota. He is a member of the California, North Carolina, and District of Columbia bars.

I. Introduction

Every surfer dreams of getting barreled at Trestles or walking the nose on the long right-hander waves at San Onofre. It would also be ideal to surf a spot on Oahu with Waikiki's relaxing waves while being the only one on the peak or catching a "sunset sesh" on Kauai. For surfers, especially those in the military or their families, these experiences are possible because all of these surfing options are available on military installations.[1] These surf breaks are vital because of the benefit they provide to service members and families as well as the economic value they bring to the community. Many reefs near the shoreline of some military installations also provide a recreational venue for SCUBA divers. From a legal standpoint, preserving these surfing breaks and diving locations on and near Department of Defense (DoD) installations is imperative to fulfill the DoD's obligations under the National Environmental Policy Act, Clean Water Act, Coastal Zone Management Act, and National Historic Preservation Act. Additionally, sustaining surf breaks implicates public policy matters and is vital to maintaining positive relations with the community. The DoD must act proactively by considering these resources in its use and development of military installations and by preserving these sites as important cultural and natural resources. Federal installations need to prepare for coastal and marine spatial planning to become more prevalent in the coming years. Coastal and marine spatial planning will be useful for ensuring protection of ocean recreational resources and resolving compatibility of offshore energy development with mission considerations and resource preservation.

This article begins by exploring the importance of preserving surfing and diving resources on DoD installations. Next, it will discuss the benefits and shortcomings of current preservation authorities such as the National Environmental Policy Act, Clean Water Act, Coastal Zone Management Act, and National Historic Preservation Act, and how the DoD should approach these laws relating to surfing and diving resources. Finally, the article will discuss coastal and marine spatial planning as an avenue to proactively preserve these resources and how the DoD should proceed going forward.

II. Background

Surfing breaks are unique because they are a rarity in the world. Most beach areas are not suitable for surfing.[2] Suitable areas must have good water quality, and there must be suitable wave quality, known as "surfability;" therefore, surfing is limited to much smaller areas than open-water swimming.[3] Surfability requires a specific combination of underwater topography, sediment, swell, and beach direction to generate waves useful for surfing.[4] Additionally, only certain locations have

the proper wind direction and intensity (usually light, offshore winds) to make for decent surf conditions.[5] When a surf break is eliminated, or conditions deteriorate such that the waves are lower quality, the lost break cannot be replaced.[6]

While the number of surfers has swelled, the number of surfing breaks has diminished to make way for ocean development.[7] While the true number of surfers is hard to quantify, studies indicate that there are upwards of 2.5 million surfers in the United States.[8] Participation in the sport is growing at a rapid pace, with an estimated 40 percent increase in the number of surfers between 2004 and 2016.[9]

SCUBA diving is a more recent development than surfing. The technology that allowed for breathing underwater that we use today was developed during World War II.[10] Navy SEALs specialize in SCUBA diving as part of their training at the Naval Special Warfare Training Center near Coronado, California,[11] and SCUBA diving is a prominent recreational opportunity at Naval Station Guantanamo Bay, Cuba.[12] According to studies by a diving trade association, there are approximately 3 million active divers in the United States and about 11 million snorkelers.[13] Many service members or their family members take part in these activities.

A. The Military's Relationship to Surfing

While SCUBA diving was developed by the military,[14] is a skill currently used in some special operations career fields, and is a popular recreational activity, the military has in the past had a more contentious relationship with surfing. Several quality surfing breaks are on military installations. In California, there are surfing beaches located at Vandenberg Air Force Base (near Point Conception), Naval Base Ventura County (Point Mugu), Camp Pendleton (northern San Diego County), Naval Air Station North Island (southern San Diego County) and Naval Station Coronado (southern San Diego County).[15] In Hawaii, Marine Corps Base Hawaii, Coast Guard Air Station Barbers Point, Pililaau Army Recreation Center, and Joint Base Pearl Harbor-Hickam all host surfing spots on Oahu, with similar waves to the famed Waikiki, but without the crowds.[16] On Kauai, the Barking Sands Pacific Missile Range Facility also features a surf break.[17] On the Atlantic coast, Naval Station Mayport, Coast Guard Station Ponce Inlet, and Patrick Air Force Base in Florida all have good surfing opportunities.[18] Several other bases in coastal locations have surfing breaks close to the installation. These surfing breaks provide a morale and recreation benefit to the service members and their families stationed at those locations.

The military's current relationship to surfing breaks has improved over historical approaches. One prime example of military action that destroyed surf breaks was the installation of the breakwater to protect the port of Long Beach and the Navy fleet during World War II.[19] In the 1940s, two sections of breakwater were constructed to complement a seawall at the mouth of the San Pedro harbor. At the time, Long Beach had been a popular surfing location. Its waves were compared to Waikiki, the gentle, rolling waves in Hawaii, and it even hosted a world surfing tournament.[20] However, with the construction of the Long Beach breakwater, the result was an end to Long Beach's surfing; in addition to creating diminished water quality from the poor circulation.[21]

At Joint Base Pearl Harbor-Hickam, construction of the Reef Runway in the 1970s also likely destroyed surfable waves.[22] Honolulu International Airport and Joint Base Pearl Harbor-Hickam share the use of the Reef Runway.[23] The Air Force, Army, and Navy donated land from Hickam Air Force Base to support the project.[24] The Reef Runway was built offshore on top of a coral reef complex.[25] The Navy had operated a recreational beach facility at the location that had to be closed.[26] The water in this area had already been polluted by prior military dredging activities and wastewater discharge.[27] Given the pollution, and that the recreational use of the reef was limited to activities "requiring only a minimum of contact with the water," the use of the reef for surfing was not analyzed in the Environmental Impact Statement.[28] The project was opposed by environmental groups, who unsuccessfully sought an injunction on the basis that the Environmental Impact Statement insufficiently assessed the environmental impact of the offshore runway construction.[29] The Reef Runway used by Joint Base Pearl Harbor-Hickam represents an example of a coral reef habitat and likely reef surfing break that was initially degraded with military use and later outright destroyed.[30] A small reef surfing break on Joint Base Pearl Harbor-Hickam, known as Hickam Beach, remains to the west of the Reef Runway.[31]

Current approaches to surfing and diving resources are more ambivalent. While the policy of the DoD and military services is that mission always comes first, the military services support the use of DoD property for recreational activities when it does not conflict with mission purposes.[32] Of the military bases that have surfable waves, Camp Pendleton's use of the coastal area is the most intensive because the Marine Corps focuses on amphibious operations and conducts training there.[33] However, the cobblestone bottom of Trestles and San Onofre makes the location exquisite for surfers but not amenable to training, so the impact of training activities in the location is minimal.[34] Trestles has been prioritized for recreational use since President Richard Nixon brokered a lease with California to operate the coastal area as a state park in 1971.[35] That 50-year lease will expire in 2021.[36] This

military surfing amenity provides a significant benefit to the economy of the town of San Clemente, which neighbors the surf breaks.[37] One example of the military's recognition of the importance of this resource is through environmental analysis prior to major federal actions on Camp Pendleton.[38] For example, when the Marine Corps acquired and implemented use of a new amphibious assault vehicle, they analyzed the impact to Camp Pendleton's surfing breaks.[39] The Marine Corps' recognition of the importance of maintaining surfing breaks while accomplishing their mission highlights that the approaches taken by military installations are vital to the preservation of surfing and diving resources located on their coastlines.[40]

B. Causes of Degradation of Surfing and Diving Resources

Ocean development is not the current proximate cause of the wholesale destruction of entire surfing breaks at many locations. Surfing breaks are also affected by the degradation of water quality from other ocean uses and water pollution from shore-based stormwater runoff.[41] What is unique to surfing as opposed to swimming and diving is the fact that surfing breaks are affected by differences on the ocean bottom (bathymetry) from changed sedimentation flows from creeks and the nearshore environment, which causes alterations to the waves.[42]

Construction along the coast, such as coastal development or coastal armoring projects, usually has a negative impact on sediment flows and bathymetry at a surfing location.[43] Human impact through development along a watershed also changes the flows of sediment in the nearshore environment.[44] Development that encroaches on streams or creeks inland causes erosion that leads to the wrong kind of sediment flowing out to the ocean that would not otherwise be present.[45] While the effect on diving resources is indirect, altering the ecosystem of the diving environment, the effect on surfing is direct because it affects the quality of the waves.[46] Conversely, development projects such as dams also prevent sediment that provides natural beach nourishment from reaching the ocean.[47] Integrated coastal zone management is needed to protect surfing breaks from impacts generated by onshore development.[48]

In addition, all water contact users are impacted by water quality from both a human health and an aesthetic standpoint.[49] Thus, poor water quality or bacteria in the water from urban runoff or petroleum spills also impacts surfers and can result in the closure of surfing areas.[50] Additionally, advisories are commonly issued to warn recreational users not to enter the water for 72 hours following a rain event.[51] Diving is best conducted in areas that have a vibrant underwater ecosystem, such as reefs and kelp forests. Healthy underwater ecosystems draw recreational users to those areas for diving and snorkeling. Conversely, poor water quality will also cause

an area to become unsuitable for diving activities.[52] Water quality has improved in recent years with major upgrades to sewage treatment in urban areas, which reduces pollutant discharge.[53] However, water quality continues to remain a concern.

C. Economic Impact of Diving and Surfing Resources on Local Communities

In discussing the need for greater protection of ocean resources for water-contact recreational uses, it is important to quantify the economic impact that those resources present to the economy.[54] The pragmatic, quantifiable economic impact on a coastal community from a surfing or diving location will sway the level of public involvement in the project that impacts the surfing or diving amenity, rather than intrinsic arguments such as the need for recreation or conservation of the environment.[55]

Diving and surfing resources provide strong economic benefits to coastal communities. Divers spend money on equipment, training, parking, food, lodging, and guide services.[56] Based on information published by the Diving Equipment and Marketing Association (DEMA), average direct expenditures per dive ranged between $116 and $234.[57] Snorkeling trip expenditures average between $44 and $100 per snorkeling trip.[58] A 2011 study estimated that there were 3.3 million surfers in the United States who represented an overall economic benefit of $2 billion.[59]

When iconic surfing location Trestles, located on Camp Pendleton, was threatened by the proposed extension of the 241 Toll Road in South Orange County, researchers performed a study to quantify the impact that the surfing break brings to the town of San Clemente, CA.[60] They determined that surfers at Trestles produced a direct economic contribution of $8-12 million for the town of San Clemente in the form of "restaurants, shopping, gasoline, rentals, and other beach-related incidentals" that then result in "jobs, wages, salaries, and taxes" that would not occur but for the surfing resource.[61] The surfing area of Trestles has an economic value of between $21 million to $45 million.[62] Communities also receive revenue from parking fees at surfing locations and other coastal recreational activities that are accrued during a surfing trip.[63] The Trestles study provides insight into the economic impact created by a single surfing location and provides the economic impetus for the preservation of the resource. Preserving surf breaks also promotes property values and tax revenues.[64] With the ever-increasing numbers of surfers and divers in America and the economic benefit these resources provide to local communities,[65] military installations can expect to face public scrutiny for actions that impact those resources.

III. Discussion

Several laws have components protecting surfing and diving resources on or near military installations. These laws impose various penalties when the installation takes action contrary to the law, which includes injunctions to stop a project or monetary fines. The primary federal laws that address coastal development on military installations are the National Environmental Policy Act, the Clean Water Act, and the Coastal Zone Management Act.[66] The National Marine Sanctuaries Act and the National Historic Preservation Act also have some limited application when discussing recreational resources.

A. Current Applicable Authorities

1. National Environmental Policy Act

An overarching statute that provides essential coastal and marine spatial planning authority is the National Environmental Policy Act. This statute requires review and public comment for federal actions (such as permitting decisions) that lead to significant environmental impact.[67] For every major federal action, such as constructing a new building or converting a land parcel from one use to another, the federal agency proposing the action must provide a statement addressing the environmental impacts of the action and alternatives to the action.[68] Per the Air Force's Environmental Impact Analysis Process regulations, where there is the "[p]otential for significant degradation of the environment" or "[s]ubstantial environmental controversy" over the impact of an action, an environmental impact statement is required.[69] Otherwise, an environmental assessment is required unless the action is categorically excluded from analysis and will have a "minimal adverse effect on environmental quality."[70]

The federal agency proposing the action must consult with other agencies that have "jurisdiction by law or special expertise with respect to any environmental impact involved."[71] Some states have laws that operate in parallel with the National Environmental Policy Act, such as the California Environmental Quality Act, which requires an assessment of environmental impacts.[72] Environmental analysis documents prepared under the National Environmental Policy Act can also serve as the assessment required under state law provided that the requirements of both state and federal law are met in the same document.[73] Additionally, for actions that affect surfing or diving resources, coastal installations should consult with the state's Ocean Policy Committee and comparable state authorities, such as the California Coastal Commission or California's Ocean Protection Council.[74]

In practice, federal installations have not been consulting with all of these agencies.[75] However, failure to consult and thus failure to consider environmental impacts could lead to an environmental group or citizen obtaining an injunction against the proposed activity.[76] Thus, to fulfill the National Environmental Policy Act requirements, military installations should consult with appropriate agencies for actions that may affect surfing or diving resources.

The National Environmental Policy Act provides a useful tool for citizens and environmental groups to ensure that federal agencies are analyzing and disclosing environmental impacts; however it only goes so far to protect environmental resources. The National Environmental Policy Act does not require a federal agency to select the least harmful alternative to the environment.[77] The regulations implementing the National Environmental Policy Act require agencies to provide an opportunity for public comment and to respond to public comments.[78] Involved citizens reviewing a project can and will publicly comment throughout the process.[79] If their concerns are not addressed, they may sue to ensure that the agency considered all of the environmental impacts.[80] Citizens and environmental groups are occasionally successful in obtaining an injunction against agency proposals, such as military training activities.[81]

For example, where a coastal and marine spatial plan exists, "Federal agencies consider environmental impacts" on the uses designated within such plans.[82] For instance, if a coastal seawall is proposed, then the federal agency would have to consider the impact on nearby marine reserves or recreational uses. Failure to respond to comments or failure to fully analyze environmental impacts could lead to environmental groups or private citizens suing to obtain an injunction to prevent implementation of the agency's proposal.[83]

However, the National Environmental Policy Act does not prevent the implementation of a project that would negatively impact the environment.[84] As long as a federal agency implementing an action analyzed the impact that an action would have on a surfing break or diving location, the agency can still select the option that destroys the resource.[85] As a result, the National Environmental Policy Act has shortcomings as a reliable tool to protect surfing and diving resources. Nevertheless, it provides powerful incentives to ensure that federal agencies fully analyze the environmental impacts that an action will have.[86]

2. Clean Water Act

The Clean Water Act, signed into law in 1972, addresses two sources of water pollution: discharge of pollutants into waterways and dredging or filling, especially

in wetlands.[87] The primary goal of the Clean Water Act is to ensure that the nation's waters are fishable and swimmable, which would be a water quality level suitable for surfing and diving.[88]

a. Section 402 – Discharge of Pollutants from Point Sources

Section 402 of the Clean Water Act regulates the discharge of pollutants from point sources into waters of the U.S.[89] This law requires permits for discharges into regulated waters, which is the most commonly treated wastewater from sewage.[90] A permit is also required and mitigation measures must be followed for construction sites disturbing more than one acre of land.[91] Discharge permits require the permit-holder to use certain technology to achieve cleaner discharges as well as maintain overall water quality.[92] For a wastewater treatment plant to receive a discharge permit, the facility needs to meet standards to be able to clean pollutants from the effluent.[93] If the discharge is determined not to meet water quality standards, then the discharge source is subject to penalties.[94] Standard enforcement is largely delegated to the states, with the EPA exercising overall supervision. Almost all states have been granted authority by the EPA to manage the wastewater discharge-permitting program.[95] Additionally, most states are granted authority to regulate federal facilities.[96]

About half of military installations operate wastewater treatment facilities on the installation.[97] Of the installations with surfing or diving resources, only Camp Pendleton has on-site wastewater treatment, and it uses advanced standards of treatment.[98] Other installations with surfing and diving resources send their sewage off the installation for treatment by local municipal facilities.[99] Installations that use wastewater treatment located upstream from surfing or diving resources, such as Eglin Air Force Base, can also affect the water quality downstream.[100]

Overall, the Clean Water Act has been successful at reducing water pollution from industrial point sources and sewage treatment facilities. In Southern California, which contains many world-famous surfing breaks, "water quality has improved dramatically since implementation" of the Clean Water Act.[101] However, water pollution from urban stormwater runoff, which is not regulated by the Clean Water Act, continues to be a problem.[102] While stormwater runoff is still an issue for military installations, it is much less of an issue for military installations than for urban communities at large because most military installations have less concentrated use of land.[103]

b. Section 404 – Dredging and Fill Permit Requirements

Section 404 of the Clean Water Act regulates the disposition of dredged materials into regulated waters or construction of breakwaters.[104] Under the definitions of the Clean Water Act, a "vessel" is considered a point source.[105] Items such as "dredged spoil," "sand," or "rock" are considered to be pollutants.[106] This does not prevent the construction of new breakwaters or depositing dredged material into waters, but it does require obtaining a permit.[107] The permitting process requires a public hearing before issuing a permit.[108]

The most evident application of Section 404 is that it imposes a requirement to obtain a permit before filling a wetland.[109] While wetlands are not useful in themselves for surfing or diving, they provide important water quality functions.[110] Wetlands promote proper sediment flows downstream to surfing and diving locations, which promotes bathymetry for surf spots and ecosystem growth in dive spots.[111]

The Army Corps of Engineers grant permits in most states, and the applicable regional or local water board must certify that the permit complies with the state's water quality plan.[112] Permits cannot be granted to fill a wetland if it there are "significantly adverse effects" on "recreational, aesthetic, and economic values."[113] To obtain a wetlands fill permit, the developer must provide mitigation in the form of restoring wetlands within the same watershed.[114] If citizens or environmental organizations find that Clean Water Act permitting provisions are administered improperly, they have the standing to raise legal challenges.[115]

The Clean Water Act applies to federal facilities, such as military installations, in much the same way that it applies to nongovernmental facilities.[116] Federal facilities may be subject to injunctions to enforce compliance with Clean Water Act provisions. Additionally, citizens have the standing to sue to enforce federal agencies' compliance with the Clean Water Act.[117] While sovereign immunity exempts federal agencies from civil penalties or punitive fines for Clean Water Act violations, agencies may still face monetary sanctions.[118] Still, this provides an effective method for citizens' groups to ensure that wastewater discharge from military installations is within allowable standards.

3. Coastal Zone Management Act

The federal Coastal Zone Management Act was also signed into law in 1972. Coastal states are required to identify coastal uses that degrade water quality and implement plans to control coastal land use and development to promote water

quality.[119] All coastal states currently participate in the national Coastal Zone Management program.[120] The main application of this law to activities on military installations is that "each federal activity within or outside the coastal zone that affects any land or water use or natural resource of the coastal zone shall be carried out in a manner consistent" with the state's coastal zone management program.[121] Within 90 days of final approval of a federal activity, such as a Record of Decision under the National Environmental Policy Act, the federal agency must provide the state with a determination that the federal activity is consistent with the state's coastal zone management plan.[122]

This law provides a powerful avenue for states to protect surfing and diving resources because federal agency actions are required to be consistent with state regulation of the coastal zone, "to the maximum extent practicable."[123] Where there is a disagreement between state regulations and the federal agency's activity, the law provides for mediation as an alternative to litigation.[124] The President holds the authority to determine that federal action is in the "paramount interest of the United States" and exempts a non-consistent activity from state regulation.[125]

The Coastal Zone Management Act exempts federal lands from the definition of the coastal zone.[126] As such, coastal installations such as Vandenberg Air Force Base that fall under exclusive federal jurisdiction would not be considered in the coastal zone per the statute.[127] However, under the Federal Consistency Program, coastal installations are required to comply with the Coastal Zone Management Act when the federal action has "spillover impacts" that affect land use, water use, or natural resources of the coastal zone outside of the federal land.[128] Federal actions must be consistent with the state's coastal zone management plan.[129] In instances where a federal installation's jurisdiction and ownership extends to the mean high tide line, the surf break or diving reefs would be outside of the federal ownership because they are further out. Thus, this law can be used by states to regulate federal activities on installations that may have an impact on the coastal recreational resources. The main limitation on using this law to protect recreational resources is the law provides enforcement authority to the states and not to private citizens or environmental groups.[130] Additionally, under the Coastal Zone Management Act, where there is a disagreement between the state and federal government over whether a federal action will have a detrimental impact on the coastal zone, the Commerce Department provides mediation services to resolve the difference.[131] The Coastal Zone Management Act, while helpful, is not a complete defense to recreational resources, so surfers and divers are at the mercy of the state's approach to recreational resources and the importance that the state places on them.

a. California

To meet the federal Coastal Zone Management Act requirements in California, the California Coastal Commission created the California Coastal Management Plan, which was approved by the National Oceanic and Atmospheric Administration (NOAA) in 1978.[132] Salient for divers and surfers, the California Coastal Act provides that "[c]oastal areas suited for water-oriented recreational activities that cannot readily be provided at inland water areas shall be protected for such uses."[133] The Coastal Commission at a minimum has jurisdiction within 1,000 yards of the coastline; however, it may extend up to the lesser of "the first major ridgeline" or "five miles from the mean high tide line of the sea" in "significant coastal estuarine, habitat, and recreational areas."[134] The Coastal Commission also has jurisdiction over the state's three-mile territorial jurisdiction out to sea.[135] Development within the Coastal Zone requires a permit.[136] The California Coastal Act places various priorities on uses of oceanfront land.[137] Recreational facilities have priority over non-coastal dependent uses "but not over agriculture or coastal-dependent industry."[138]

When the Coastal Commission or municipalities are issuing permits for development or other activities under the Coastal Management Plan, the statute provides the opportunity for public comment.[139] The public comment process provides concerned citizens, including recreational ocean users, an important tool to be involved in new coastal development or freeway construction that impacts surf breaks or diving locations.[140] There are also litigation options available to citizens and environmental organizations against state agencies.[141] For example, through lengthy litigation and a resulting settlement, regular Trestles surfers were able to force the California Department of Transportation to take into account the sedimentation impact on Trestles caused by the extension of the 241 Toll Road near San Clemente.[142] While this litigation did not involve the DoD, this example is illustrative of the litigation pitfalls that DoD installations could face when engaging in construction or training activities that affect recreational sites.

b. Hawaii

In Hawaii, the Office of Planning administers the state's Coastal Zone Management Program.[143] Hawaii's coastal zone encompasses the entire state.[144] The rationale for this is an understanding that "[w]hat occurs on land, even on the mountains, will impact and influence the quality of the coastal waters and marine resources."[145] Despite being the birthplace of surfing, the Hawaii Coastal Zone Management Act's language protecting recreational uses is not as strong as the California Coastal Act. The Hawaii Coastal Zone Management Act requires agencies

to "give full consideration to ecological, cultural, historic, esthetic, recreational, scenic, and open space values, and coastal hazards, as well as to needs for economic development."[146] Hawaii has ocean planning policies that set forth priorities and provide for conservation areas but stops short of marine spatial planning.[147] The Hawaiian law provides for private citizens and environmental groups to initiate lawsuits against agencies not in compliance with the Coastal Zone Management Act.[148] Ultimately, the federal government is not bound by any state's decision, but could be brought to mediation to resolve differences.[149]

c. Florida

Florida has an approved Coastal Management Plan to fulfill the requirements of the federal Coastal Zone Management Act.[150] The Florida Coastal Management Plan is codified into 24 separate statutes.[151] Florida's coastal zone provisions generally extend 1,500 feet inland from the shoreline. For barrier islands (which is where surfing breaks are located in Florida), the coastal zone provisions apply 5,000 feet inland.[152] Construction in the coastal zone is required to "be located a sufficient distance landward of the beach to permit natural shoreline fluctuations and preserve dune stability."[153] The requirements for building projects within the coastal zone focus on structures being able to withstand coastal storms and flooding.[154] The Florida Coastal Management Plan provides for permitting for rigid coastal armoring structures to protect beachfront property from erosion and storms.[155] While the Florida statute mentions recreational resources, its language is not as strong as California's Coastal Act. The Florida statute expresses the intent of the legislature that "[o]pportunities must be increased to provide natural resource-based recreation" and "coastal areas are among Florida's most valuable resources and have an extremely high recreational and aesthetic value which should be preserved and enhanced."[156] However, by the state's terms, only some of Florida's Coastal Management Program is not enforceable against federal agencies for purposes of consistency determinations.[157]

4. Marine Protected Area Networks

The most comprehensive conservation mechanism for ocean areas are federal and state Marine Protected Areas. Marine Protected Areas are designed to protect "natural and cultural resources."[158] There are various types of Marine Protected Areas that provide varying levels of protection for marine mammals within their boundaries.[159]

Five requirements must be met when the Commerce Secretary designates a location as a Marine Protected Area.[160] The first requirement is that the protected area will fulfill the purposes of the National Marine Sanctuaries Act, which includes marine conservation and ecosystem management.[161] The second requirement is the protected area is of "special national significance" based on "conservation, recreational, ecological, historical, scientific, cultural, archaeological, educational, or esthetic qualities; the communities of living marine resources it harbors; or its resource or human-use values."[162] The third requirement is that existing authorities "are inadequate or should be supplemented" to ensure "comprehensive conservation and management."[163] The fourth requirement is the National Marine Sanctuary designation will "facilitate the objectives" of comprehensive conservation and management, scientific research, and public education.[164] Finally, the "size and nature" of the protected area must "permit comprehensive and coordinated conservation and management."[165]

Although recreational use is a permissible reason to designate a Marine Protected Area, the current network has focused on ecological conservation.[166] Federal Marine Protected Areas are integrated into a combined system with state Marine Protected Areas.[167] Marine Protected Areas serve a vital function in protecting resources.[168] Typically, diving is prevalent in areas where they exist.[169] By comparison, few surfing areas are located within Marine Protected Areas.[170] Although Marine Protected Areas are not on federal installations, they do exist under military airspace over the ocean.[171] Thus, Marine Protected Areas provide a helpful function in preserving diving resources in some areas.[172] Military installations need to consider Marine Protected Areas in conducting training activities, but these protected areas have minimal impact on other activities on the installation.

5. National Historic Preservation Act

While the Coastal Zone Management Act and Marine Protected Areas provide governmental regulation to promote conservation of the marine environment, historical preservation is another avenue that has been used to protect surfing resources. Historical preservation is assured by listing a location on the National Register of Historic Places (National Register).[173] When a location is listed on the National Register, any proposed federal agency action requires the agency to consult with the State Historic Preservation Office or the Advisory Council on Historic Preservation and integrate measures developed during consultation into making a decision.[174] Despite this requirement, "decisions rest with the agency implementing the undertaking."[175] The only surf break currently listed on the National Register of Historic Places is Malibu, listed as a historic district.[176]

Listing a surfing resource on the National Register is difficult. Few surf breaks qualify for the rigid criteria.[177] Even if the surf breaks on DoD installations could qualify, there could be other obstacles, such as the need for the DoD to certify the listing of resources on military bases.[178] For example, the Trestles surfing break failed to achieve registration on the National Register despite nomination.[179] Although the Trestles surfing break met the criteria for historic preservation, the Navy refused to certify the application because of the potential for conflict with the training needs of Camp Pendleton.[180] While the option of historic preservation has been tried as a method to provide preservation for surfing breaks, it provides more leverage to the DoD than it does to surfers.[181] Historic preservation is only an effective avenue to preserve surfing breaks if the military installation wants to pursue listing an eligible surfing resource.[182] For example, historic preservation may provide some protection to diving locations on military installations if the diving location contains a historic artifact such as an airplane or shipwreck.[183]

In summary, the National Environmental Policy Act, the Clean Water Act, the Coastal Zone Management Act, Marine Protected Area Networks, and the National Historic Preservation Act provide a significant layer of protection for surfing and diving resources on or near DoD installations. DoD installations need to take their responsibilities under these statutes seriously. These statutes provide avenues for citizen lawsuits, and they can also result in injunctions preventing military missions against installations that fail to follow their provisions as it relates to surfing or diving resources.

B. Coastal and Marine Spatial Planning to Protect Recreational Resources

Federal installations should be prepared for coastal and marine spatial planning to become more prevalent in the coming years, which could provide significant additional protections for surfing and diving spots on or near DoD installations.[184] The states of Massachusetts, Rhode Island, and Washington have implemented coastal and marine spatial planning, and several other states such as Hawaii and California have shown interest in the concept.[185] Most coastal states are also members of larger regional planning bodies.[186] Coastal and marine spatial planning efforts in New Zealand and Australia, which focus on providing protections for ocean recreational resources such as surfing and diving locations, also provide specific examples of coastal and marine spatial planning that could be applied domestically.[187]

Coastal and marine spatial planning applies concepts of zoning used to regulate land use onto the ocean's use.[188] Coastal and marine spatial planning is a two-part process that consists of information gathering and then developing an ocean-zoning scheme.[189] The process allocates permitted uses of ocean spaces "based on a determination of an area's suitability for those uses" and reduce conflicts "by separating incompatible activities."[190] Planners consider outside influences that affect the areas to be zoned.[191] Planners also identify complementary uses of various areas and the intensity of uses permissible in those areas.[192] Once the permissible uses and intensity of those uses have been determined, the planners would then issue regulations that govern those uses, enforcement mechanisms to ensure compliance, and incentives to promote voluntary compliance.[193] The coastal component of coastal and marine spatial planning involves studying and regulating onshore activities in the coastal zone that impact the oceans.[194] Coastal and marine spatial planning is dynamic and thus adaptable to changing conditions, such as seasonal rotation of uses or whale migration patterns.[195] Coastal and marine spatial planning follows a cyclical approach, meaning that once a plan is developed, it is then reviewed and can later be revised as new information becomes available.[196]

Coastal and marine spatial planning is a process that contemplates stakeholder interests, designates uses for particular areas of the ocean, and continuously evaluates the uses based on data.[197] Environmental stakeholder groups, such as the Surfrider Foundation, have a greater ability compared to the current legal framework to actively contribute to the planning process and ensure that planners follow the law's requirements.[198] The involvement of stakeholder organizations in a coastal and marine spatial planning context differs from public comment procedures utilized under other environmental laws.[199] Typical comment procedure involvement is responsive to an individual project or proposal.[200] Within coastal and marine spatial planning, stakeholders are supposed to be involved from the outset with the overall planning process, cutting across multiple sectors.[201] This is a far more active level of engagement than currently exists with typical public comment procedures.[202] Planners would work with stakeholders to identify and prioritize areas that are important to recreational users.[203] Additionally, if planners stray from the legal requirements, these stakeholder groups can serve an important enforcement role by filing citizen suits to induce compliance.[204]

Planners can also import parts of successful initiatives from other areas of the world such as Australia, New Zealand, and Europe and modify them, as necessary, to fit the needs of the planning area.[205] Additionally, coastal and marine spatial planning can take into account new and evolving technologies that can provide more effective protections for recreational sites and ocean ecology. For instance, California comprehensively mapped its territorial waters.[206] From a recreational

standpoint, this data revealed important bathymetric features to surfing breaks such as Mavericks near Santa Cruz, California.[207] This data can be used to better develop a plan to protect these resources.

Coastal and marine spatial planning allows planners to study areas that are used for recreational water-contact uses and study the primary threats that those areas face, both internally and externally. From there, the planners can develop regulations to preserve those areas and balance the interests competing for ocean and coastal uses.[208] A coastal and marine spatial planning program could regulate onshore development as well, by encompassing an area a certain distance from water features, such as rivers that flow into the ocean, an approach taken by Rhode Island.[209]

1. Current Legal Framework for Coastal & Marine Spatial Planning

At the federal level, several statutes provide federal agencies with authority to regulate the various parts that form a coastal and marine spatial plan.[210] However, absent an overarching statutory scheme, there are shortcomings in that coastal and marine spatial planning would have to be implemented on a segmented basis, with different portions of the planning effort developed by different agencies.[211]

Statutes at the federal level include the National Marine Sanctuaries Act, which provides current authority for designating Marine Protected Areas.[212] Additionally, the Antiquities Act authorizes the designation of National Monuments.[213] National Monuments can be quite large, as in the case of the Papāhanaumokuākea Marine National Monument in Hawaii.[214] However, creating a National Monument is more complicated than a Marine Protected Area because it requires Presidential action.[215] Finally, the Endangered Species Act and Marine Mammal Protection Act can be used specifically to protect critical habitats for threatened and endangered species and marine mammals, respectively.[216] These Acts each build in significant protection for wildlife, and monuments and the areas that surround them that can be incorporated into coastal and marine spatial planning.[217]

Despite statutory authority to implement aspects of coastal and marine spatial planning, a shortcoming of the current federal statutory scheme is that each statute is very sector-specific.[218] Successful coastal and marine spatial planning efforts at the federal level would require at least twenty different federal agencies to work together.[219] The National Ocean Policy Committee (which replaced the National Ocean Council in 2018) could be able to serve in the role of a coordinating body to implement coastal and marine spatial planning among the agencies that are empowered with pieces of marine spatial planning.[220]

At the state level, there is much greater latitude to implement coastal and marine spatial planning under the auspices of the state's police powers.[221] For instance, in California, the California Coastal Act governs a large amount of the aspects of coastal and marine spatial planning.[222] California's Marine Life Protection Act governs conversation areas for sea life as well as fishing regulations.[223] California also created the Ocean Protection Council as a coordinating and information-sharing body among agencies that is useful for coastal and marine spatial planning efforts.[224] The Ocean Protection Council also oversees California's Marine Protected Area system.[225] One of California's Ocean Protection Act mandates is to provide the Ocean Protection Council as the coordinating body for scientific data for agencies to implement coastal and marine spatial planning.[226]

2. Resolving Compatibility of Different Ocean Uses

Coastal and marine spatial planning recognizes there are competing uses of the ocean that can have a detrimental impact on ecology and recreational sites. Coastal and marine spatial planning can also mitigate the detrimental impact of pollution and changed sediment flows that coastal development presents to ocean recreational sites.[227] Under coastal and marine spatial planning, existing ocean structures would be dismantled if they no longer served the purpose for which they were originally needed.[228] For example, the Long Beach breakwater has outlived its purpose in creating a safe harbor for naval vessels.[229] Using Coastal and marine spatial planning, this type of obsolete ocean development would be removed in a manner protective of this natural resource to promote more important recreational use.[230] Coastal and marine spatial planning would provide a comprehensive set of tools that planners can use to protect recreational ocean sites through controls on other ocean activities and appropriate vetting and limitations on development in coastal watersheds.

Coastal and marine spatial planning offers military installations an important tool to resolve mission compatibility with offshore energy development. For example, offshore wind energy development is major focus of the Biden administration.[231] However, offshore wind power generation presents concerns for mission accomplishment as well as detrimental effects on surfing resources.[232] From a mission standpoint, a collection of wind turbines creates a blind spot for radar, preventing effective navigation of aircraft, ships, and rockets.[233] Offshore wind turbines can have negative effects on surfing breaks because they affect wave height and coastal sediment flow, which in turn affects wave shape.[234] One alternative energy source that has fewer negative impacts on navigation and may have fewer impacts on surfing wave quality is wave energy generation.[235] Marine Corps Base Hawaii-Kaneohe has been an instrumental partner with Department of Energy

and industry to support testing and development of wave energy power generation facilities.[236] Coastal and marine spatial planning would provide a mechanism for military installations to resolve mission and environmental concerns to offshore energy development and ensure offshore energy siting with minimal impacts.

As state jurisdiction only extends to three nautical miles from the coastline, integration with the federal government is necessary to ensure comprehensive coastal and marine spatial planning.[237] This conflict can be resolved through the Federal Consistency Program of the Coastal Zone Management Act.[238] Thus, federal installations need to plan for the move towards comprehensive coastal and marine spatial planning, and should take ocean uses into account when preparing environmental reports under the National Environmental Policy Act and making consistency determinations under the Coastal Zone Management Act.

IV. Conclusion

Surfing and diving resources on or near DoD installations represent tremendous morale and recreational benefits for service members and their families. These surfing breaks and diving locations also have a strong economic impact on the coastal communities near them. The National Environmental Policy Act, Clean Water Act, Coastal Zone Management Act, and the network of Marine Protected Areas provide substantive protection to these resources that DoD installations need to be aware of in order to follow the statutory requirements. DoD installations also need to be prepared for further regulation in this area in the form of coastal and marine spatial planning. Specifically, coastal and marine spatial planning provides a way for military installations to ensure compatibility of offshore energy projects with mission accomplishment and protection of recreational resources. Not only do these resources provide a strong recreational and economic benefit that deserves protection, but there are also legal consequences in failing to follow statutory requirements. By ensuring that DoD installations follow the requirements and prioritize the preservation of surfing and diving resources when conducting activities on the installation, these installations will be able to successfully protect these valuable resources.

Endnotes

[1] Jon Anderson, *Best Military Surf Spots: Exclusive Beaches in 5 Hubs*, Mil. Times (Aug. 12, 2015), *available at* https://www.militarytimes.com/off-duty/2015/08/12/best-military-surf-spots-exclusive-beaches-in-5-hubs/.

[2] Scott Ball, *The Green Room: A Surfing-Conscious Approach to Coastal and Marine Management*, 33 UCLA J. Envtl L. & Pol'y 366, 369-70 (2015); Chad Nelsen, Andy Cummins, and Hugo Tagholm, *Paradise Lost: Threatened Waves and the Need for Global Surf Protection*, 1 J. Coastal Res. 904 (No. 65, 2013) (noting that "surfers are extremely particular about their beach choice based on numerous oceanographic, meteorological, surf, and social conditions. As a result, environmental impacts such as water quality impairment or changes in beach processes from coastal development will likely impact the beach choice, and thus the economic values and contributions of surfers differently than other beachgoers").

[3] For a discussion of factors that make for a "surfable" wave, *see* Ball, *supra* note 2, at 369-373.

[4] *Id.* at 369-70.

[5] *Id.*

[6] *Id.* at 382.

[7] Edwin C. Kisiel, *A Southern California Surfer's Perspective on Marine Spatial Planning*, 31 Villanova Envt'l L.J. 225, 230, 235 (2020).

[8] *Id*. at 230.

[9] *Id*.

[10] *SCUBA Diving,* Marine Bio Conservation Soc'y, https://marinebio.org/creatures/tools/scuba-diving/ (last visited Mar 22, 2021).

[11] *BUD/S (Basic Underwater Demolition/SEAL) Training*, NAVYSEALS.com, https://navyseals.com/nsw/bud-s-basic-underwater-demolition-seal-training/ (last visited Feb. 11, 2021).

[12] *SCUBA,* Naval Station Guantanamo Bay, https://www.cnic.navy.mil/regions/cnrse/installations/ns_guantanamo_bay/ffr/things_to_do/recreation/scuba.html (last visited Feb. 11, 2020).

[13] Diving Equipment & Marketing Association (DEMA), Fast Facts: Recreational SCUBA Diving and Snorkeling (2018), *available at* https://www.dema.org/store/download.aspx?id=7811B097-8882-4707-A160-F999B49614B6 (last visited Mar. 22, 2021).

[14] Dave Chace, *Dr. Christian Lambertsen: 70 Years of Influence on the Military Dive Community*, Army.mil (15 March 2012), *available at* https://www.army.mil/article/75716/dr_christian_lambertsen_70_years_of_influence_on_the_military_ddiv_community (discussing invention of SCUBA for the U.S. military during World War II).

[15] Jon Anderson, *supra* note 1; *Gator Beach*, WannaSurf.com, https://www.wannasurf.com/spot/North_America/USA/California/San_Diego_County/gator_beach/index.html (last visited Feb. 5, 2020) (discussing the beach on Coronado where the Navy SEALs train); *Breakers Beach at Naval Air Station North Island*, California Beaches.com, https://www.californiabeaches.com/beach/breakers-beach/ (discussing surfing at NAS North Island) (last visited Mar. 22, 2021).

[16] Jon Anderson, *supra* note 1; *Pokai Bay Surf Forecast and Surf Reports (Oahu, USA)*, Surf Forecast.com, https://www.surf-forecast.com/breaks/Pokai-Bay (last visited 23 April 2021).

[17] *Id*.

[18] *Id*.

[19] Martin Wisckol, *Removal of Long Beach Breakwater Could be on the Rocks*, Orange County Register, Jun. 20, 2018, https://www.presstelegram.com/2018/06/20/removal-of-long-beach-breakwater-could-be-on-the-rocks/.

[20] *Id*.

[21] *Id*.; *see also 2017-2018 Beach Report Card,* Heal the Bay, 60-61 (2018), https://healthebay.org/wp-content/uploads/2018/07/BRC_2017-2018_07-12-18.pdf (describing Long Beach's current water quality to be decent (A-B range) in dry summer weather but poor in dry winter weather and wet weather).

[22] Allan Sommarstrom, Enhancement of Coastal Recreational Opportunities: A Description of Present Coastal Recreational Usage, Constraints, Data and Research Possibilities in the State of Hawaii 39 (1975), *available at* https://www.govinfo.gov/content/pkg/CZIC-ht393-h3-t42-no-6/html/CZIC-ht393-h3-t42-no-6.htm (citing John Kelly, Surf Parameters Final Report 192–210 (1973). *See also*, *HNL 1970s*, Hawaii Aviation: An Archive of Historic Photos and Facts, http://aviation.hawaii.gov/airfields-airports/oahu/honolulu-international-airport/hnl-1970s/ (last visited Feb. 6, 2020).

[23] *Id*.; Federal Aviation Administration, Final Environmental Impact Statement for Honolulu International Airport 21 (1972), *available at* http://oeqc2.doh.hawaii.gov/EA_EIS_Archive/1972-01-DD-OA-FEIS-Honolulu-Airport-Reef-Runway-8r-26l.pdf.

[24] *Id*. at 3.

[25] *Id.* at 11; *HNL 1970s*, *supra* note 22.

[26] Federal Aviation Administration, *supra* note 23, at 16.

[27] Federal Aviation Administration, *supra* note 23, at 16-17.

[28] Federal Aviation Administration, *supra* note 23, at 16.

[29] *Life of the Land v. Volpe*, 363 F. Supp. 1171, 1175-76 (1972). *See* 40 C.F.R. Part 1502 (2020) (promulgating requirements on preparation of Environmental Impact Statements under National Environmental Policy Act requirements, codified at 42 U.S.C. § 4332 (1975)).

[30] Sommarstrom, *supra* note 22, at 39.

[31] Jon Anderson, *supra* note 1. Because this spot is under the flight path and near the outlet of Pearl Harbor, surfers at Hickam Beach face more aircraft noise and water pollution impacts than other spots on Oahu, so this spot is not favored by many surfers.

[32] U.S. Dep't of Def., Instr. 4715.03, Natural Resources Conservation Program, Encl.3, ¶ 7.a (2018). *See, e.g.*, MCB Camp Pendleton, Marine Corps Integrated Natural Resources Management Plan (2017), 1-16.

[33] *See* MCB Camp Pendleton, Environmental Impact Statement for the Advanced Amphibious Assault Vehicle 4.6-1–4.7-3 (Oct. 2002) [hereinafter Amphibious Assault Vehicle EIS] (discussing impacts on land use and recreation from amphibious training).

[34] Dashel Pierson, *Could Trestles Close to the Public?*, Surfline, Apr. 28, 2017, https://www.surfline.com/surf-news/the-lease-for-san-onofre-state-beach-from-marine-corps-base-camp-pendleton-ends-in-2021/1276 (last visited Nov. 11, 2018).

[35] *See* California Office of Historic Preservation, National Register of Historic Places Registration Form 16-17 (draft). *See also*, Everett Holles, *Embattled Marines Yield a Beach in California to Sunbathers and Surfers*, N.Y. Times, Apr. 5, 1971, *available at* https://www.nytimes.com/1971/04/05/archives/embattled-marines-yield-a-beach-in-california-to-sunbathers-and.html (accessed Oct. 25, 2018); Pierson, *supra* note 34 (discussing that before Nixon arranged for the lease to California, surfers would trespass onto the base and avoid Marine patrols to use the waves). As an interesting side note, Pres. Nixon's "Western White House," La Casa Pacifica in San Clemente, overlooked the surf breaks at Trestles, and Pres. Nixon often walked the beach at the spot. Robert Nedelkoff, *Memories of President Nixon's Western White House*, Richard Nixon Foundation (Sept. 7, 2013), https://www.nixonfoundation.org/2013/09/memories-president-nixons-western-white-house/; *see also* David Morris, *Surfing in Nixonland*, N.Y. Times, Sept. 6, 2016, *available at* https://www.nytimes.com/2016/09/06/opinion/surfing-in-nixonland.html?_r=1. For the stories of the conflicts between surfers and Marines before the lease, *see generally*, Steve Pezman, *Capers in the Key of "T*," 7 Surfer's J. 74 (1998).

[36] Pierson, *supra* note 34.

[37] Chad Nelsen, Collecting and Using Economic Information to Guide the Management of Coastal Recreational Resources in California 197-98 (2012) (unpublished Ph.D. dissertation, UCLA) (*available at* http://public.surfrider.org/files/nelsen/Nelsen_2012_CA_beachsurfecon_dissertation.pdf); Chad Nelsen, Linwood Pendleton, and Ryan Vaughn, *A Socioeconomic Study of Surfers at Trestles Beach*, 75 Shore & Beach 32, 35-36 (2007).

[38] For the legal requirements of environmental analysis under the National Environmental Policy Act, *see* 42 U.S.C. § 4332 (1975); 40 C.F.R. Part 1502 (2020).

[39] Amphibious Assault Vehicle EIS, *supra* note 33, at 4.6-1–4.7-3.

[40] Jon Anderson, *supra* note 1. *See* U.S. Dep't of Def., Instr. 4715.03, Natural Resources Conservation Program, Encl.3, ¶ 7.a (2018) (providing that services should make recreational resources on the installation available to the general public when feasible).

[41] Kisiel, *supra note* 7, at 237.

[42] Chad Nelsen, *Protecting Ocean Recreation and Surfing*, Surfrider Found (Mar. 20, 2013); B.E. Scarfe, et. al., The Science of Surfing Waves and Surfing Breaks – A Review, (Mar. 7, 2003) at 6, *available at* https://escholarship.org/content/qt6h72j1fz/qt6h72j1fz.pdf (discussing the rarity of a quality surfable wave because of the need for interesting bathrythmic features). For a scientific discussion, *see* Andrew Short, *Coastal Processes and Beaches*, 3 Nature Education Knowledge 15 (2012), *available at* https://www.nature.com/scitable/knowledge/library/coastal-processes-and-beaches-26276621 (accessed Mar. 27, 2021); Edward Anthony, *Sediment-Wave Parametric Characterization of Beaches*, 14 J. of Coastal Res. 347 (1998). *See also* Tony Butt, Surf Science: An Introduction to Waves for Surfing 52-54 (3d ed. 2014) (discussing how the contour of the ocean floor affects wave formation).

[43] Nicholas Corne, *The Implications of Coastal Protection and Development on Surfing*, 25 J. Coastal Res. 427, 431-32 (2009), (analyzing the detrimental effect that most coastal armoring projects have on surfing wave quality); B.E. Scarfe, et. al., *Sustainable Management of Surfing Breaks – An Overview*, 1 Reef J. 44, 58 (2009) (discussing an erosion control project at the Chevron refinery in El Segundo, CA).

[44] Shane Anderson, *Environmental Characteristics of Malibu*, in Malibu: World Surfing Reserve 13, 13 (2010).

[45] *See, e.g.*, Stanley Trimble, *Contribution of Stream Channel Erosion to Sediment Yield from an Urbanizing Watershed*, 278 SCIENCE 1442 (1997), 1442-44 (discussing measurement of sediment yield through the Newport Bay watershed and resulting effects); *see also* Erin Nelson and Derek Booth, *Sediment Sources in an Urbanizing, Mixed Land-Use Watershed*, 264 J. HYDROLOGY 51, 61 (2002).

[46] Kisiel, *supra* note 7, at 238; Nelsen, *Protecting Ocean Recreation and Surfing*, *supra* note 42. *See also* BUTT, *supra* note 42.

[47] Anderson, *supra* note 44, at 13.

[48] Scarfe, et. al., *Sustainable Management of Surfing Breaks*, *supra* note 43, at 44.

[49] *See* Benjamin Arnold, et. al., *Acute Illness Among Surfers After Exposure to Seawater in Dry- and Wet-Weather Conditions*, 186 AM. J. EPIDEMIOLOGY 866 (2017); Katie Day, *Surfrider & UCLA Collaborate on Surfer Antibiotic Resistance Study!*, SURFRIDER, Oct. 29, 2018, *available at* https://www.surfrider.org/coastal-blog/entry/surfrider-ucla-collaborate-on-surfer-antibiotic-resistance-study (discussing ongoing research into pathogen exposure that surfers face at Los Angeles beaches due to urban stormwater runoff from development).

[50] HEAL THE BAY, *supra* note 21; *Frequently Asked Questions*, COUNTY OF ORANGE HEALTH CARE AGENCY (2019), *available at* https://ocbeachinfo.com/faq/#1460419230216-0a77e3da-dc90 (last visited Mar. 27, 2021).

[51] *Frequently Asked Questions*, COUNTY OF ORANGE HEALTH CARE AGENCY (2019), *available at* https://ocbeachinfo.com/faq/#1460419230216-0a77e3da-dc90 (last visited Mar. 27, 2021).

[52] *See* Kisiel, *supra* note 7, at 231.

[53] *See* Michael Foster and David Schiel, *Loss of Predators and the Collapse of Southern California Kelp Forests: Alternatives, Explanations, and Generalizations*, 393 J. EXPERIMENTAL MARINE BIOLOGY & ECOLOGY 59, 63-64, 66 (2010) (discussing recovery of kelp forest beds near Los Angeles and San Diego after improvements in water quality following water treatment system upgrades such as discharge further offshore into deeper waters, but sedimentation may still have adverse effects). *See also* 33 U.S.C. § 1362(6) (2021) (defining a pollutant as "dredged spoil, solid waste, incinerator residue, sewage, garbage, sewage sludge, munitions, chemical wastes, biological materials, radioactive materials, heat, wrecked or discarded equipment, rock, sand, cellar dirt and industrial, municipal, and agricultural waste discharged into water").

[54] Kisiel, *supra* note 7, at 239.

[55] Ball, *supra* note 2, at 398-99 (discussing how "economic value … is most likely to resonate with the general public and our society's decision-makers" regarding whether to proceed with development when it impacts a surfing resource).

[56] Kisiel, *supra* note 7, at 239.

[57] *Id*.

[58] *Id*.

[59] Gregory Thomas, *Surfonomics Quantifies the Worth of Waves*, THE WASHINGTON POST, Aug. 24, 2012, *available at* https://www.washingtonpost.com/surfonomics-quantifies-the-worth-of-waves/2012/08/23/86e335ca-ea2c-11e1-a80b-9f898562d010_story.html (last visited Mar. 27, 2021).

[60] Nelsen, Collecting and Using Economic Information, *supra* note 37, at 196-97; Nelsen, Pendleton, and Vaughn, *supra* note 37. *See also Landmark Agreement Ends 15-Year Dispute Over SR 241 Toll Road Extension*, Transportation Corridor Agencies (Nov. 10, 2016) *available at* https://thetollroads.com/news/newsroom/press-release/820 [hereinafter *Landmark Agreement*].

[61] Nelsen, Pendleton, and Vaughn, *supra* note 37, at 35-36.

[62] Nelsen, Pendleton, and Vaughn, *supra* note 37, at 35-36; Nelsen, Collecting and Using Economic Information, *supra* note 37, at 7, 51. Economic value is distinguished from direct economic impact because economic value represents the "net value added to society that the resource provides." *Id*. at 8. Economic value also quantifies the value of the ability to continue to use a resource, the ability to preserve a resource for future generations, or the sheer existence of the resource. *Id*. at 8-9.

[63] Nelsen, Collecting and Using Economic Information, *supra* note 37, at 7-8.

[64] Thomas, *supra* note 59.

[65] Thomas, *supra* note 59; *see, e.g.,* Nelsen, Collecting and Using Economic Information, *supra* note 37, at 196-97; *Landmark Agreement*, *supra* note 60.

[66] The National Environmental Policy Act is codified at 42 U.S.C. §§ 4321, et. seq. The Clean Water Act's Wetland Fill Permitting Requirements are found at 33 U.S.C. § 1344. The Coastal Zone Management Act is codified at 16 U.S.C. § 1455b.

[67] 42 U.S.C.S. § 4332 (1975).

[68] *Id*.

[69] 32 C.F.R. § 989.16 (2011) (The regulations at 32 C.F.R. Part 989 implement the Air Force's Environmental Impact Analysis Process under the National Environmental Policy Act.).

[70] 32 C.F.R. § 989.14 (2011); 32 CFR § 989.13 (2011). For a list of Air Force categorical exclusions, *see* 36 C.F.R. Part 989, Appendix B (2011).

[71] 40 C.F.R. § 1508.5 (2019).

[72] Cal. Pub. Res. Code § 21003 (2021).

[73] *Compare* 42 U.S.C. §§ 4321, et. seq. *with* Cal. Pub. Res. Code § 21003 (2021).

[74] *See* Exec. Order No. 13840, 83 Fed. Reg. 24931 (Jun. 19, 2018) (changing the National Ocean Council to the Ocean Policy Committee); Cal. Pub. Res. Code § 35615 (2019) (creating California's Ocean Protection Council).

[75] *See, e.g.*, Department of the Navy, Santa Margarita River Conjunctive Use Project Environmental Impact Statement 8-1 (2014); 30th Space Wing, Final Draft Environmental Assessment: 13th Street Bridge Replacement at the Santa Ynez River Crossing at 131 (2015) (showing that consultations are happening with Fish and Wildlife Service, National Marine Fisheries Service, State Historic Preservation Office, and federally-recognized tribes, and other state and federal agencies, but not all of the agencies who would be stakeholders in coastal recreational resources).

[76] William S. Eubanks II, *Damage Done? The Status of NEPA After* Winter v. NRDC *and Answers to Lingering Questions Left Open by the Court*, 33 Vt. L. Rev. 649, 657 (2009).

[77] *Id.* at 651; *NEPA Environmental Review Requirements*, Environmental & Energy Law Program (Aug. 15, 2018), https://eelp.law.harvard.edu/2018/08/nepa-environmental-review-requirements/.

[78] 40 C.F.R. § 6.203 (2020).

[79] 40 C.F.R. § 1501.5 (2019); 40 C.F.R. § 1501.6 (2021); 40 C.F.R. § 1051.9 (2021).

[80] *See, e.g.*, Davis Mts. Trans-Pecos Heritage Ass'n v. U.S.A.F., 249 F. Supp. 2d 763, 769 (2003) (alleging that the Air Force failed to take into account noise levels for expanding bomber training range over plaintiffs' lands).

[81] *See, e.g.*, Washington County, N.C. v. U.S. Dep't of the Navy, 357 F. Supp. 2d 861, 878 (2005) (county and citizens' groups obtained an injunction against the Navy because the Navy failed to properly analyze environmental impacts to waterfowl and wetlands as a result of proposed new training airspace and construction of a landing strip in North Carolina).

[82] National Ocean Council, Legal Authorities Relating to the Implementation of Marine Spatial Planning 3 (2011), *available at* https://tethys.pnnl.gov/sites/default/files/publications/Legal_Authorities_Relating_to_CMSP.pdf.

[83] *See, e.g.*, Nat'l Audubon Soc'y v. Dep't of the Navy, 422 F.3d 174 (4th Cir. 2005); Or. Nat. Res. Council v. Marsh, 832 F.2d 1489 (9th Cir. 1987); Minn. Pub. Int. Res. Group v. Butz, 358 F. Supp. 584 (D. Minn. 1973), aff'd 498 F.2d 1314 (8th Cir. 1974); Habitat Educ. Ctr. v. Bosworth, 381 F. Supp. 2d 842 (E.D. Wis. 2005).

[84] *NEPA Environmental Review Requirements*, *supra* note 77.

[85] *Id.*

[86] Eubanks, *supra* note 76, at 651–52.

[87] 33 U.S.C. §§ 1251, et. seq. (2021).

[88] 33 U.S.C. § 1251 (2021).

[89] 33 U.S.C. §§ 1311, et. seq. (2021).

[90] 33 U.S.C. § 1311 (2021).

[91] 40 C.F.R. § 122.26 (2021).

[92] 33 U.S.C. § 1316; *see* 40 C.F.R. § 125.3 (2021); 40 C.F.R. § 125.123 (2021).

[93] 40 C.F.R. §§ 125.1, et. seq. (2021).

[94] 33 U.S.C. § 1319 (2021).

[95] *NPDES State Program Information*, EPA, *available at* https://www.epa.gov/npdes/npdes-state-program-information (last visited Mar. 27, 2021).

[96] *Id*.

[97] Judith A. Barry, Characterization of DoD Installation Wastewater Treatment 1 (2012).

[98] *Id*. at D-1

[99] *Id*. at C-4–C-6.

[100] *Id*. at C-1.

[101] Greg S. Lyon & Eric D. Stein, How Effective Has the Clean Water Act Been at Reducing Pollutant Mass Emissions to the Southern California Bight over the Past 35 Years? 8-9 (2008), *available at* http://ftp.sccwrp.org/pub/download/DOCUMENTS/AnnualReports/2007AnnualReport/AR07_001_012.pdf

[102] *Id*. at 10; *See also* Kisiel, *supra note* 7, at 233–34.

[103] *See, e.g.*, U.S. Dep't of def. & U.S. Fish & Wildlife Service, Conservation Lands as Compatible Use Buffers (2004), *available at* https://www.fws.gov/endangered/esa-library/pdf/Buffer_Lands_Fact_Sheet_dec05.pdf.

[104] 33 U.S.C. § 1344 (2021).

[105] 33 U.S.C. § 1362(14) (2021).

[106] 33 U.S.C. § 1362(6) (2021).

[107] 33 U.S.C. § 1344 (2021).

[108] *Id*.

[109] *Id*.

[110] Australian Government – Department of the Environment, Wetlands and Water Quality 1 (2016), *available at* https://www.environment.gov.au/system/files/resources/b7cd579b-89b0-4602-9ba8-118b4f55ab84/files/factsheet-wetlands-water-quality.pdf.

[111] *Id*.

[112] *See, e.g.*, California Water Boards, Water Board Function: Wetlands Protection, and Dredge & Fill Regulation, *available at* https://www.waterboards.ca.gov/board_reference/majorfunctions/dredge_fill.pdf (last visited Mar. 27, 2021).

[113] 40 C.F.R. § 230.10(c)(4) (2021).

[114] 33 C.F.R. § 332.3(b) (2021).

[115] *See, e.g.*, Surfrider Found. v. Cal. Reg'l Water Quality Control Bd., 211 Cal. App. 4th 557 (Cal. Ct. App., 4th Dist., 2012) (unsuccessfully alleging that proposed mitigation measures were inadequate to minimize the impact on sea life).

[116] 33 U.S.C. § 1323 (2021).

[117] 33 U.S.C. § 1365 (2021); N.Y. v. U. S., 620 F. Supp. 374 (E.D.N.Y. 1985).

[118] 33 U.S.C. § 1323 (2021) (requiring federal facility compliance with process and sanctions for control and abatement of water pollution); U.S. Dep't of Energy v. Ohio, 503 U.S. 607, 626 (1992) (defining process and sanctions under 33 U.S.C. § 1323).

[119] 16 U.S.C. § 1455b (2021).

[120] *About the National Coastal Zone Management Program*, Office for Coastal Management (Mar. 27, 2021) https://coast.noaa.gov/czm/about/

[121] 16 U.S.C.§ 1456 (2021).

[122] *Id*.

[123] *Id*.

[124] *Id*.

[125] *Id*.

[126] 16 U.S.C. § 1453 (2021).

[127] *Id*.

[128] 15 C.F.R. § 923.33 (2021).

[129] *Id*.

[130] 16 U.S.C. § 1456 (2021).

[131] 15 C.F.R. § 930.44 (2021). *See also*, Lopez v. Cooper, 193 F. Supp. 2d 424, 428–29 (D.P.R. 2002) (discussing a CZMA dispute between the Navy and Puerto Rico over training activities).

[132] California Coastal Commission, Description of California's Coastal Management Program, *available at* https://www.coastal.ca.gov/fedcd/ccmp_description.pdf (last visited Mar. 27, 2021). The California Coastal Act of 2976 is codified at Cal. Pub. Res. Code §§ 30000, et. seq. (2021).

[133] Cal. Pub. Res. Code § 30220 (2021). While the statute does give standing for citizen suits, it appears to have been seldom used. In the one case where Surfrider Foundation sued the Coastal Commission, the dispute was not related to an environmental issue but rather the restriction of access to public beaches due to the installation of parking meters. Surfrider Found. v. Cal. Coastal Comm., 26 Cal. App. 4th 151, 154-55 (Cal. Ct. App., 5th Dist., 1994). This provision could be used more widely for citizens' suits to challenge coastal development and marine uses that interfere with swimming and diving activities. *See* Cal. Pub. Res. Code § 30801 (2021) (permitting citizen suits in cases where the plaintiff or a representative "appeared at a public hearing" or provided public comments).

[134] Cal. Pub. Res. Code § 30103(a) (2021). The Coastal Commission also overlaps with federal lands, such as at Camp Pendleton. For maps, *see Maps: Coastal Zone Boundary*, California Coastal Commission, https://www.coastal.ca.gov/maps/czb/ (last visited Mar. 27, 2021). *See also* Cal. Pub. Res. Code §§ 30150-74 (2021) (codifying adjustments to Coastal Zone boundaries on case-by-cases bases).

[135] 43 U.S.C. § 1301 (2021) (providing for state jurisdiction to three miles out from coastline); Cal. Pub. Res. Code § 30103(a) (2021).

[136] Cal. Pub. Res. Code §§ 30600, et. seq. (2021).

[137] Cal. Pub. Res. Code §§ 30221, et. seq. (2018).

[138] Cal. Pub. Res. Code § 30222 (2021).

[139] Cal. Pub. Res. Code § 30006 (2021).

[140] Kisiel, *supra* note 7, at 244.

[141] Cal. Pub. Res. Code § 30803 (2021).

[142] David Zimmerle, *Another Twist in Trestles Toll Road Saga*, Surfer (Aug. 21, 2017), https://www.surfer.com/features/another-twist-in-trestles-toll-road-saga/ (last visited Mar. 27, 2021); *Landmark Agreement*, *supra* note 60.

[143] *Hawaii CZM Program*, State of Hawaii Office of Planning, http://planning.hawaii.gov/czm/about-czm/ (last visited Mar. 27, 2021).

[144] Haw. Rev. Stat. § 205A-1 (2021).

[145] *Hawaii CZM Program*, *supra* note 143.

[146] Haw. Rev. Stat. § 205A-4 (2021).

[147] *See, e.g.*, Hawaii State Office of Planning, Hawai'i Ocean Resources Management Plan 68-73 (2013), *available at* http://files.hawaii.gov/dbedt/op/czm/ormp/ormp_update_reports/final_ormp_2013.pdf.

[148] Haw. Rev. Stat. § 205A-6 (2021).

[149] Lopez v. Cooper, 193 F. Supp. 2d 424, 429 (D.P.R. 2002).

[150] *About the Florida Coastal Management Plan*, Fla. Dep't of Envtl Prot. (Jan. 12, 2021, 12:46 PM), https://floridadep.gov/rcp/fcmp/content/about-florida-coastal-management-program (last visited Mar 27, 2021).

[151] *Id.*

[152] Fla. Stat. § 161.054(1) (2020); Fla. Stat. § 161.55(4) (2020).

[153] Fla. Stat. § 161.055 (2020).

[154] *Id.*

[155] Fla. Stat. § 161.085 (2020).

[156] Fla. Stat. § 161.72 (2020); Fla. Stat. § 161.53 (2020).

[157] *See* Office of Resilience and Coastal Protection, Florida Coastal Management Program Guide 13 (2020), *available at* https://floridadep.gov/sites/default/files/FCMP_Program_Guide_Aug_2020.pdf (listing policies which are and are not enforceable against federal agencies).

[158] Nat'l Oceanic & Atmospheric Admin. & Dep't of The Interior, Framework for the National System of Marine Protected Areas of the USA (2015), at 4, *available at* https://nmsmarineprotectedareas.blob.core.windows.net/marineprotectedareas-prod/media/archive/nationalsystem/framework/final-mpa-framework-0315.pdf [hereinafter NOAA, Framework] (last visited Mar. 27, 2021).

[159] *Id. at 4.* (noting that Marine Protected Areas provide "an array of levels of protection and conservation purposes, from areas that allow multiple-use activities to areas that restrict take and/or access").

[160] 16 U.S.C. § 1434 (2021).

[161] 16 U.S.C. § 1433(a)(1) (2021). The Act's purposes are set forth at 16 U.S.C. § 1431(b) (2019).

[162] 16 U.S.C. § 1433(a)(2) (2021).

[163] 16 U.S.C. § 1433(a)(3) (2021).

[164] 16 U.S.C. § 1433(a)(4) (2021).

[165] 16 U.S.C. § 1433(a)(5) (2021).

[166] NOAA, Framework, *supra* note 158, at 12-13.

[167] NOAA, Framework, *supra* note 158, at 5.

[168] *Compare* Cal. Dep't of Fish & Wildlife, California South Coast Marine Protected Areas (Oct. 1, 2014), *available at* https://nrm.dfg.ca.gov/FileHandler.ashx?DocumentID=105397&inline, *with Snorkeling Santa Barbara*, *Central California*, Gone Snorkeling, *available at* https://www.gonesnorkeling.com/destinations/usa/california/santa-barbara/ (last visited Mar. 27, 2021) *and Dive Sites – Southern California*, Beach Cities Scuba, https://www.beachcitiesscuba.com/pages/dive-sites (last visited Feb. 15, 2020). Many prime diving spots, boasting healthy rocky-reef kelp forest ecosystems, are also within state or federal Marine Protected Areas.

[169] Kisiel, *supra* note 7, at 248.

[170] *Compare* Cal. Dep't of Fish & Wildlife, *supra* note 168, *with California Surf Reports & Cams*, Surfline, https://www.surfline.com/surf-reports-forecasts-cams/united-states/california/5332921 (last visited Mar. 27, 2021) (showing the location of surf spots in California on the interactive map).

[171] *See, e.g.*, Amec Foster Wheeler, Inc., Environmental Impact Statement for Proposed Establishment and Modification of Oregon Military Training Airspace G-15–G-17 (2015). *Compare* United States Air Force, United States Military Installations, Ranges, Special Use Airspace, and Military Training Routes (2021), *available at* https://catalog.data.gov/dataset/military-installations-ranges-and-training-areas *with* National Marine Protected Area Center, *NOAA's MPA Inventory*, U.S. Marine Protected Areas, https://marineprotectedareas.noaa.gov/dataanalysis/mpainventory/mpaviewer/ (last visited Mar. 27, 2021).

[172] Kisiel, *supra* note 7, at 248.

[173] *See* 54 U.S.C. § 302102 (2021) (providing for listing of property that meets statutory criteria on the National Register of Historic Places).

[174] 36 C.F.R. § 60.2(a) (2021); 36 C.F.R. § 800.3 (2021); 36 C.F.R. § 800.4 (2020).

[175] 36 C.F.R. § 60.2(a) (2021).

[176] *See* 83 Fed.Reg. 2668 (Jan. 18, 2018) (soliciting comments on the proposed listing of beach area from Malibu pier to Malibu Colony); *Malibu Historic District*, National Park Service, https://www.nps.gov/places/malibu-historic-district.htm (last visited Mar. 27, 2021).

[177] Ball, *supra* note 2, at 402. Listing criteria that would be relevant for surfing breaks requires "quality of significance in American history … and culture" to be "present in districts, sites … that possess integrity of location … setting … feeling, and (a) that are associated with events that have made a significant contribution to the broad patterns of our history, or (b) that are associated with the lives of persons significant in our past …." 36 C.F.R. § 60.4 (2018). Additionally, properties generally must have "achieved significance" at least 50 years prior to listing on the National Register. 36 C.F.R. § 60.4 (2018). *See also*, California Office of Historic Preservation, National Register of Historic Places Registration Form 7, *available at* (providing justification for Trestles to be listed on the National Register of Historic Places despite having achieved significance within the last 50 years).

[178] 36 C.F.R. § 60.6(y) (2021) (discussing that nominations are submitted to the federal agency that owns the property for review and comment).

[179] *See* Michael Blum, Protecting Surf Breaks and Surfing Areas in California 35-36 (May 2015) (unpublished master's thesis) (on file with Duke University's Nicholas School of the Environment), *available at* https://hdl.handle.net/10161/9592 (last visited Mar. 27, 2021) (discussing the failure of nomination for Trestles because of failure of Dep't of the Navy to certify the nomination); Monica Garske, *Navy, Marines Oppose Historic Nomination for Trestles Beach*, NBC 7 San Diego (9 February 2013), *available at* https://www.nbcsandiego.com/news/local/camp-pendleton-marines-navy-oppose-historic-designation-for-trestles-beach-san-onofre/2078069/.

[180] Monica Garske, *Navy, Marines Oppose Historic Nomination for Trestles Beach*, NBC 7 San Diego (9 February 2013), *available at* https://www.nbcsandiego.com/news/local/camp-pendleton-marines-navy-oppose-historic-designation-for-trestles-beach-san-onofre/2078069/.

[181] Kisiel, *supra* note 7, at 250.

[182] *Id*.

[183] *See* 36 C.F.R. § 60.4 (2021).

[184] Kisiel, *supra* note 7, at 270–72.

[185] *Id*.

[186] *United States of America (National)*, Marine Spatial Planning Programme, http://msp.ioc-unesco.org/world-applications/americas/us/national/ (last visited 26 April 2021) (discussing Northeast, Mid-Atlantic, West Coast, and Pacific Islands regional planning organizations).

[187] Kisiel, *supra* note 7, at 267–70.

[188] Tundi Agardy, Ocean Zoning: Making Marine Management More Effective 7 (2010).

[189] John M. Boehnert, Zoning the Oceans: The Next Big Step in Coastal Zone Management 66-67 (2013).

[190] Agardy, *supra* note 188, at 7–8.

[191] *See, e.g.*, 650 R.I. Code.R. § 20-05-11.10.1 (2021) (discussing considerations in the citing of offshore wind energy sites as it relates to impacts within the coastal area). *See also* Blue Earth Consultants, Coastal and Marine Spatial Planning Background Document 14 (2011), *available at* https://www.oregonocean.info/index.php/ocean-documents/planning/marine-spatial-planning/922-coastal-and-marine-planning-and-california-california-ocean-protection-council-july-12-2011/file (last visited Mar. 27, 2021).

[192] Agardy, *supra* note 188, at 7–8.

[193] *See* Agardy, *supra* note 188, at 45–46.

[194] Boehnert, *supra* note 189, at 141.

[195] Agardy, *supra* note 188, at 32; Olga Koubrak, Ph.D. candidate, Panelist on Marine Mammal Protection at the Geo. Wash. L. Sch. Conf. on Changing and Dynamic Oceans: Gauging Law & Policy Responses (Nov. 10, 2018).

[196] Agardy, *supra* note 188, at 32

[197] Agardy, *supra* note 188, at 45-46.

[198] *Ocean Protection*, Surfrider, *available at* https://www.surfrider.org/initiatives/ocean-protection (last visited Mar. 27, 2021).

[199] Cal. Pub. Res. Code § 21003 (2021).

[200] Blue Earth Consultants, *supra* note 191, at 20.

[201] Blue Earth Consultants, *supra* note 191, at 20-21.

[202] Blue Earth Consultants, *supra* note 191, at 20.

[203] *Ocean Protection*, *supra* note 198.

[204] *See, e.g.*, Surfrider Found. v. Cal. Reg'l Water Quality Control Bd., 211 Cal. App. 4th 557 (Cal. Ct. App., 4th Dist., 2012).

[205] Kisiel, *supra* note 7, at 266–70. *See e.g.*, Ball, *supra* note 2, at 386-88 (discussing how initiatives in Australia and Peru can form the basis of an approach for planners to use to protect surfing resources).

[206] Betsy Mason, *New Maps Reveal California's Sensational Seafloor Geography*, Wired (May 22, 2015), *available at* https://www.wired.com/2015/05/new-california-seafloor-maps/; Sean Greene, *Scientists Explore 2,000 Miles of the Ocean Floor – And You Can Too*, LA Times (Mar. 20, 2015), *available at* https://www.latimes.com/science/sciencenow/la-sci-sn-explore-ocean-floor-usgs-20150319-story.html.

[207] Memorandum from Daniel Santillano, Ocean Protection Council, to California Protection Council 2-3 (Aug. 27, 2014), *available at* http://www.opc.ca.gov/webmaster/ftp/pdf/agenda_items/20140827/Item6_OPC_Aug2014_Seafloor_and_Coastal_Mapping.pdf.

[208] Kisiel, *supra* note 7, at 251.

[209] Boehnert, *supra* note 189, at 141.

[210] Environmental law institute, Marine Spatial Planning in U.S. Waters, vii–viii (2009), *available at* https://www.eli.org/sites/default/files/eli-pubs/d19_13.pdf. *See also*, National Ocean Council, *supra* note 82, at 1-2.

[211] National Ocean Council, *supra* note 82, at 1-2.

[212] 16 U.S.C. § 1434 (2021). *See also*, Marine Spatial Planning in U.S. Waters., *supra* note 210, at 4-6; National Ocean Council, *supra* note 82, at 19-20.

[213] 54 U.S.C. § 320301 (2021).

[214] 54 U.S.C. § 320301(b) (2021) ("The limits of the parcels shall be confined to the smallest area compatible with the proper care and management of the objects to be protected."). *See* National Ocean Council, *supra* note 82, at 19-20 (discussing legal authority for establishing National Monuments in the ocean and the large size of some of the National Marine Monuments).

[215] *Compare* 16 U.S.C. § 1434 (2019) (specifying Secretary of Commerce as authority to designate areas of national significance) *with* 54 U.S.C. § 320301 (specifying the President as the authority to designate National Monuments).

[216] 16 U.S.C. § 1533(a)(3)(A) (2021) (providing for the designation of critical habitat under the Endangered Species Act); 16 U.S.C. § 1382(e) (2019) (providing for the development of conservation measures to alleviate impacts on marine mammal "rookeries, mating grounds, or areas of similar ecological significance"). *See also*, Marine Spatial Planning in U.S. Waters, *supra* note 210, at 7-9.

[217] Marine Spatial Planning in U.S. Waters, *supra* note 210, at 7-9.

[218] National Ocean Council, *supra* note 82, at 1.

[219] *See* Boehnert, *supra* note 189, at 114.

[220] Fact Sheet: Donald J. Trump is Promoting America's Ocean Economy, Trump White House Archives (June 19, 2018), https://trumpwhitehouse.archives.gov/briefings-statements/president-donald-j-trump-promoting-americas-ocean-economy/?utm_source=twitter&utm_medium=social&utm_campaign=wh (last visited Mar. 27, 2021).

[221] U.S. Const. amend. X ("The powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people."). *See, e.g.*, Cal. Pub. Res. Code §§ 30200, et. seq. (2019); Blue Earth Consultants, *supra* note 191, at 36-39, 43-45.

[222] Cal. Pub. Res. Code § 30600 (2019).

[223] Cal. Fish & G. Code § 2860 (2019).

[224] Cal. Pub. Res. Code § 35615 (2019).

[225] Cal. Fish & G. Code § 2850.5 (2019).

[226] Cal. Pub. Res. Code § 35620 (2019).

[227] Kisiel, *supra* note 7, at 275–77.

[228] *See, e.g.,* New Zealand Coastal Policy Statement 2010, Policy 6: Activities in the Coastal Environment, § 2.e.ii.(2010) (requiring "removal of any abandoned or redundant structure that has no heritage, amenity or reuse value").

[229] Wisckol, *supra* note 19.

[230] *Long Beach Breakwater*, Surfrider Found. Long Beach, https://longbeach.surfrider.org/breakwater/ (last visited 26 April 2021).

[231] Exec. Order. No. 14008, *Tackling the Climate Crisis at Home and Abroad*, § 207 (Jan. 27, 2021) (expressing goal of doubling offshore wind energy production by 2030).

[232] Kisiel, *supra* note 7, at 256.

[233] *Id*.

[234] Tony Butt, *Will New Windfarm Ruin One of Europe's Greatest Surfing Spots?*, Magic Seaweed (Aug. 17, 2020), https://magicseaweed.com/news/offshore-windfarms-and-their-impact-on-wave-quality/12014/; Kisiel, *supra* note 7, at 256; *see generally* Tsumoru Shintake, *Harnessing the Power of Breaking Waves*, 3 Proceedings Asian Wave & Tidal Energy Conf. 623 (2016).

[235] Butt, *supra* note 234.

[236] LCpl Brittany Vella, *Wave of the Future: Base Welcomes Newest Testing Buoy*, Marine Corps Base Hawaii (Feb. 20, 2015), https://www.mcbhawaii.marines.mil/News/News-Article-Display/Article/566806/wave-of-the-future-base-welcomes-newest-testing-buoy/; Construction Progressing on Full-Scale Triton-C, Oscilla Power (Jun. 16, 2020), https://www.oscillapower.com/post/construction-started-on-full-scale-triton-c.

[237] NOAA, Framework, *supra* note 158, at 3-4.

[238] Boehnert, *supra* note 189, at 40.

Incentivizing 'Active Debris Removal' Following the Failure of Mitigation Measures to Solve the Space Debris Problem: Current Challenges and Future Strategies

*Major Adam G. Mudge**

*Major Adam G. Mudge, USAF, (LL.M., Air and Space Law, McGill University (2020); J.D., University of Alabama School of Law (2009); B.S., Psychology & Cognitive Studies, Vanderbilt University (2006)) is the Legal Advisor to United States Space Command's Joint Task Force – Space Defense (JTF-SD), Schriever Space Force Base, Colorado. He is a member of the Alabama bar.

Introduction

A. Issues and Objectives

At the dawn of the space age and for many years thereafter, outer space was accessible only to enormous governmental civil and defense infrastructures,[1] most notably those of the United States and the former Soviet Union. Over time that exclusivity evaporated, and as of November 2020, some 9,400 satellites have been launched into Earth orbit by governmental and commercial entities, of which only about 3,000 remain operational.[2]

In addition to these functioning satellites, uncontrolled and non-operational man-made matter also exists in space. In total, approximately 23,000 space objects greater than 10 centimeters in diameter were being tracked by the United States Air Force's Space Surveillance Network (SSN) in 2018.[3] Many millions more pieces of smaller debris are estimated to be in orbit, but unobservable, and therefore untrackable, from Earth.[4] Some of this debris can be attributed to specific States, while much cannot.

En masse, these nonfunctional and uncontrolled pieces of space debris pose serious collision risks to operational satellites and manned spacecraft, as well as to the surface of the Earth, ultimately even threatening to contaminate the space environment itself. This risk, which has been acknowledged for many decades,[5] has continued to grow as the space environment has become more and more congested. In order to reduce this risk, individual States and the international community have engaged in concerted debris mitigation efforts since the early 1990s, notably via the U.S. led, multi-national creation of the Inter-agency Space Debris Coordination Committee (IADC) in 1993 and the addition of space debris as a topic on the agenda of the Scientific and Technical Subcommittee (STSC) of the United Nations (U.N.) Committee on the Peaceful Uses of Outer Space (COPUOS) in 1992.[6] However, due to significant structural limitations within resulting mitigation guidelines and poor global compliance, these efforts have done little to stop year-on-year increases in the total number and mass of objects in Earth orbit.[7] Additionally, the emergence of new space-faring nations and commercial entities, accidental collisions, in-space fragmentations, and several intentional debris-creating events, specifically direct ascent anti-satellite (ASAT) missile tests, have compounded the problem of uncontrolled debris.

It is now the conclusion of many leading space organizations, such as the European Space Agency (ESA),[8] that space-faring nations must collectively move beyond simply pursuing mitigation efforts alone and begin focusing on physically

removing some of the debris from Earth orbit or properly stabilizing and storing it in special 'graveyard' orbits, a process known as remediation or, more commonly, active debris removal (ADR).[9] However, the legacy international space law regime, primarily inherited from the 1960s and 1970s in the form of five seminal U.N. Space Treaties (the Outer Space Treaty,[10] the Liability Convention,[11] the Rescue and Return Agreement,[12] the Registration Convention,[13] and, to a lesser extent, the Moon Agreement[14]), creates special legal challenges inhibiting ADR. For example, the U.N. Space Treaties not only fail to provide a legally binding definition for what constitutes space debris, but they fail to mention debris at all. Further, there are no clearly recognized international obligations with respect to the creation nor the removal of space debris. Fundamental concepts from these treaties appear to have been drafted without envisioning a future world containing ADR space operations. For example, the "jurisdiction and control" provision in Article VIII of the OST establishes enduring, hegemonic control for States of registry over their space objects and fail to provide a mechanism for the transfer or abandonment of space objects. Further, the liability regime established by the Liability Convention disincentivizes ADR when it comes to both the owner of the piece of debris and the State wishing to carry out the ADR operation. It also fails to set out a standard of fault or to establish a mechanism for the transfer of liability. Each of these issues threatens to complicate necessary global ADR efforts. National defense concerns, economic concerns, and various national laws adopted by States since this time, notably export control laws, have further complicated the legal and policy landscapes for ADR operations.

The failure of mitigation efforts and the global need for ADR, along with the aforementioned complex legal and policy challenges, will be the focus of this article. Part I defines the scope of the problem posed by space debris thorough an analysis of its causes, its observable characteristics, and its distribution throughout the primary Earth orbits. It further explains the dangers posed by uncontrolled debris, especially in light of its significant increase over time, and concludes by highlighting several discrete contributing factors and events that have dramatically exacerbated this increase in recent years.

Part II examines the historical failure of states to craft an international space *lex lata* to rein in or even moderate the increase in space debris. It details the drafting and widespread adoption of various soft law instruments at both the national and international levels. Ultimately, it argues that these measures have failed to adequately address the dangers posed by increasing space debris, thereby justifying the critical need for ADR.

After this need for ADR has been substantiated, Part III opens by briefly explaining some of the most promising technological methods of ADR. Then it analyzes the structural and systemic international and national legal challenges which currently frustrate the efforts of governmental, inter-governmental, and non-governmental entities wishing to carry out ADR, as briefly described above. Much of this analysis focuses on either lacunae or fundamental concepts embedded within the OST and the Liability Treaty. Part III also highlights certain national laws, specifically export control laws, as well as several policy issues, such as economic costs and national security considerations, which pose similar challenges to the successful implementation of ADR.

Finally, Part IV argues for a future strategy to address the challenges raised in Part III. Specifically, it advocates for the drafting and adoption of an entirely new multinational space treaty, describing in general terms the necessary changes to current international space law which must be made to facilitate the growth of ADR operations. Some of these changes include establishing new binding international definitions and obligations related to space debris, adjusting the jurisdiction and control rules for space debris, permitting the abandonment of space debris, modifying and modernizing the current liability regime, establishing a regulatory agency in charge of space debris, and empowering such an agency to raise funds for ADR. Short of the adoption of a new space treaty, Part IV alternatively discusses a role for more limited space protocols to existing U.N. treaties. Finally, Part IV concludes by addressing the ways in which individual States can also support ADR efforts through purely national means.

B. Context and Limitations

Before launching into the body of the article, a quick note on the context of the public international space law regime is in order. Little hard law has been generated to move the ball forward on a large scale since the Registration Convention in 1974. Soft law agreements, such as memoranda of understanding, voluntary guidelines, and a slew of U.N. General Assembly (UNGA) resolutions have instead helped filled that gap.[15] During this period of legal stagnation, the technology and practical means to safely and effectively accomplish several forms of ADR have become closer and closer to being fully realized. In fact, many commercial and governmental prototypes have been patented,[16] and some have already undergone operational testing in the outer space environment.[17] Without a modern legal landscape within which to operate, the implementation of this burgeoning ADR technology will be beholden to outdated legal concepts. This context, where the rollout of technological innovation is being stifled by legal stagnation, is the backdrop for this project and its lengthy description of the current seriousness of

the space debris problem in Part I and its discussion of the challenges inhibiting ADR in Part III.

In part because of the above context, the door is open to many possible creative solutions to overcome the identified challenges and advance the efficacy of ADR within the space law landscape. However, it is worth noting here that, while Part IV suggests several desirable solutions, its intent is not to present exhaustive or fully developed legal proposals for new national and international law. In that regard, it will not propose specific definitions for space debris nor precise verbiage for a new space treaty or protocol. Such an enterprise exceeds the scope of this article. Each of the ideas presented in Part IV is merely a starting point, worthy of future research and analysis if international progress is to be made on ADR.

Finally, while the descriptions of various ADR technologies in Part III(A) highlight an impressive variability, they are not intended to be extensive nor exhaustive. Instead, they are presented merely to provide context for understanding the current challenges and future strategies presented later in Parts III and IV.

C. Terminology

It will be worthwhile to briefly comment on certain terms which will be used throughout this article. While the term "ADR" is a form of and generally synonymous with "remediation," ADR will be used as the preferred term, consistent with the prevailing usage in the literature. Also, ADR is used herein as a comprehensive term, without distinction to the many ways in which it might be conducted. For example, when discussing the jurisdiction and control of a piece of space debris during ADR, no distinction is made between conducting ADR by attaching an electrodynamic tether versus using a grappling arm. When such a distinction amongst the various methods of ADR may be relevant to the challenges discussed, such as with respect to international liability for damage if a ground-based laser is employed, it is made apparent. While the concept of on-orbit satellite servicing (OOS) can be closely related to ADR as a means of remediation, it will not be addressed in this project.[18]

The terms used to describe debris in space varies by organization. For example, the National Aeronautics and Space Administration (NASA) uses the term "orbital debris" or "micrometeoroid and orbital debris (MMOD)" while ESA employs the term "space debris." Depending on the user and the context, these terms may or may not include naturally occurring objects orbiting Earth, such as small fragments of rock or metal from meteoroids. This article will utilize the term "space debris,"

as this term is generally used in the literature to denote specifically the man-made debris orbiting Earth.[19]

Finally, in conducting ADR, it is most often the case that a space object will interact with one or more other space objects. In order to precisely identify these objects in relation to one another, the term "ADR object" or "ADR State" is used to denote the space object actively conducting the removal of a piece of space debris or the State possessing jurisdiction and control over that space object, respectively. Similarly, the term "space debris" is used to denote the targeted object of the removal action, while the term "debris State" is used to denote the State which possesses jurisdiction and control over that target.

I. Scope of the Space Debris Problem

The term "space debris" is not defined in any of the U.N. Space Treaties, nor will it be precisely defined by this article. However, both the UNGA, through its adoption of the COPUOS Space Debris Mitigation Guidelines, and the IADC by virtue of its own Space Debris Mitigation Guidelines, subscribe to the following definition: "all man-made objects including fragments and elements thereof, in Earth orbit or re-entering the atmosphere, that are non-functional."[20] Assuming this definition for purposes of discussion, grasping the scope of the space debris problem requires an understanding of where this type of debris comes from, where it is located, the dangers it poses, and how it has developed over time.

A. Causes of Space Debris

Man-made, non-functional objects in space are generated in several different ways. Most can be classified as either mission-related debris, discarded rocket bodies, fragmentation debris, microparticulate debris, or non-operational payloads.

1. Mission-Related Debris

Mission-related debris, sometimes described as operational debris, includes intentionally discarded objects due to the launch, deployment, activation, operation and de-orbit of the payload, which do not otherwise affect the integrity of the payload or launch vehicle.[21] It accounts for approximately 10-11% of all orbital space objects catalogued by the United States' Space Surveillance Network (SSN).[22] Mission-related debris most commonly includes smaller pieces of hardware intentionally released during payload deployment or operation, such as sensor or engine protective covers, straps, springs, temporary shields, or

stabilization devices.[23] Advances in technology and design have resulted in a dramatic decrease in the creation of this type of space debris since 1990.[24]

2. Discarded Rocket Bodies

This category of space debris includes the discarded upper stages of the launch vehicle used to deliver the payload into its orbit. These stages can range in mass from less than 100 kilograms to as much as eight metric tons.[25] Similar to mission-related debris, discarded rocket bodies make up between 10-11% percent of all orbital space objects currently catalogued by the SSN.[26] While typical space missions leave a single rocket body behind in Earth orbit, others may leave as many as three strewn across separate orbits.[27] Incredibly, according to NASA, roughly 30% of all launch vehicle stages used since 1957 are still in orbit,[28] totaling nearly 1,950 rocket bodies in 2018.[29]

3. Fragmentation Debris

Fragmentation debris is debris created by the breakup of rocket bodies or payloads, whether caused by an internal explosion or anomalous physical separation or by some external collision event.[30] Fragmentation debris makes up the lion's share of space objects, or approximately 53% of all objects currently catalogued by the SSN.[31] Fragmentation events are categorized as either a satellite breakup or an anomalous event, the former generally being a high velocity, destructive event with fragments breaking off in different directions and at different velocities, while the latter is typically a lower velocity, unplanned and mostly-intact separation, often due to physical deterioration of the payload in the space environment.[32] Satellite breakups most commonly result from an accidental malfunction, especially by on-board propulsion systems, or may result intentionally, for example due to ASAT weapons testing,[33] whereby States test ground or air launched anti-satellite ballistic missiles by targeting and destroying their own satellites while still in Earth orbit.

Very few known fragmentation events to date have been caused by external collisions; instead, most are caused by internal explosions or anomalous physical separations.[34] While NASA figures show that more than 320 fragmentation events have occurred since 1957,[35] ESA estimates that fewer than ten of these have been due to accidental or intentional collision events.[36] Several of these ten events will be discussed in more detail in Part I(D).

4. Microparticulate Debris

Microparticulate debris, as the names suggests, are the smallest form of space debris, ranging anywhere from micrometer dust particles to one-centimeter objects.[37] This type of debris is commonly released from solid rocket motors in the form of aluminum dioxide dust and particles.[38] It is also commonly found in the form of tiny flakes of material coatings or paint, degraded from either micro collisions or simple material deterioration from the harsh outer space environment.[39] Sodium potassium coolant liquid, once used to cool nuclear power sources, is another known cause of microparticulate debris.[40] In fact, NASA estimates that approximately 70,000-100,000 sodium potassium droplets of various sizes remain in low Earth orbit (LEO).[41] While small in size, the tremendously fast orbital velocities of microparticulate debris (up to ~10 km/s or 36,000 km/hr in the lowest orbits)[42] and the difficulty in tracking them can render them exceedingly dangerous. Because of this, NASA's Chief Scientist for Orbital Debris, Dr. Jer Chyi Liou, has categorized debris in the 1mm-1cm range as posing the highest mission-ending threat to current NASA space operations.[43]

5. Non-Operational Payloads

In addition to mission-related debris, ejected rocket bodies, fragments, and microparticulates, many defunct payloads remain in orbit, having either malfunctioned or reached the end of their useful lives. Functional and non-functional payloads together comprise just under 25% of the space objects catalogued by the SSN.[44] However, it is estimated that less than two-third of all orbiting payloads are still functional,[45] which means that roughly 2,650 non-operational payloads continue to orbit the Earth as space debris.[46] Together, these defunct satellites comprise approximately 15% of the total space objects catalogued by the SSN.[47] Some non-operational payloads are small in size and mass, but others, especially older payloads in higher orbits, can weigh several tons.[48]

B. Characteristics of Space Debris

1. Observability

Space objects are capable of being identified and tracked through the use of world-wide networks of ground-based and space-based optical telescopes and radars, the largest of which is the SSN maintained by the U.S. Department of Defense.[49] The capability of the SSN to identify and track space objects differs based on the object's orbital altitude.

LEO, a portion of outer space ranging in altitude from the lowest boundary of space, however defined, up to 2,000 kilometers above the Earth's surface, is the area where most human activities in space take place, where the International Space Station (ISS) is positioned, and where many Earth observation satellites or telescopes are maintained.[50] Powerful phased array radars are most often used to detect space objects in this region.[51] Only identified space objects in excess of roughly 10 centimeters are routinely tracked by the SSN at this altitude.[52] However, advances in technology promise to reduce the size of trackable objects in LEO significantly. For example, a $1.5 billion U.S. DoD joint venture with Lockheed Martin to build a large ground-based radar system called the "Space Fence" recently became operational on Kwajalein Atoll in the South Pacific in March 2020, and is reportedly capable of tracking objects as small as a marble in LEO.[53]

The areas in Medium Earth Orbit (MEO), or between 2,000 and approximately 35,000 kilometers above the Earth's surface, are used primarily for navigation and communication satellites.[54] Major Global Navigation Satellite Systems (GNSS) are predominantly located here, such as the United States' Global Positioning System, Russia's GLONASS, Europe's Galileo, and China's BeiDou constellations.[55] Objects above approximately 5,000 kilometers are best detected through the use of optical telescopes, such as the U.S. Ground-Based Electro-Optical Deep Space Surveillance System (GEODSS).[56] Generally, the ability to accurately track space objects in this region decreases from about 10 centimeters at the lowest regions of MEO to about one meter at the highest regions of MEO.[57]

Finally, Geostationary Orbit (GEO), or the orbits at and immediately adjacent to roughly 35,786 kilometers above the Earth's equator, are used primarily for communications and broadcasting.[58] Ideally, a graveyard orbit at least 235 kilometers above GEO is also used to dispose of satellites in this region at the end of their useful life.[59] Similar to upper MEO, objects located in GEO are best detected and tracked through the use of advanced electro-optical telescopes, although very powerful mechanical radars can also be used.[60] Generally speaking, only space objects in excess of approximately one meter are trackable by the SSN in this region.[61]

2. Quantity, Mass, and Distribution Throughout Space

In total, the SSN tracked approximately 23,000 objects in space larger than 10 centimeters in 2018.[62] However, just because the SSN *tracks* an object does not mean that the genesis of that object is known for liability, jurisdictional, or any other purposes, nor does it mean that the object is necessarily functional. In fact, the identity is only known for approximately 19,500 of these objects (such that

they have been *catalogued* by the SSN)[63] and in 2019 only about 3,000 of all tracked objects were actually functional satellites.[64] This means that well over 85% of the tracked objects in the SSN are non-functional space debris. As for operational satellites, according to the Union of Concerned Scientists in November 2018 (when there were only 1,957 in orbit), 1,232 were operated in LEO, 558 were operated in GEO, 126 were operated in MEO, and a further 41 were operated in non-standard elliptical orbits.[65] In other words, 63% of all functional satellites in November 2018 were in LEO, 28.5% were in GEO, 6.5% were in MEO, and 2% were in elliptical orbits.[66]

While the SSN may only have been actively tracking 23,000 space objects in 2018, advanced space debris modeling, such as NASA's LEGEND or ESA's MASTER,[67] as well as additional experiments conducted *in situ* and detailed analyses of recovered hardware provide insight into the volume of additional space debris *not* being tracked by the SSN, either because it is too small to track or because it has simply not yet been identified.[68] Using these models and methods, ESA estimates that, as of January 2019, more than 34,000 pieces of space debris greater than 10 centimeters in size are orbiting Earth, while a further 900,000 exist between 1 and 10 centimeters.[69] Most astonishingly, ESA estimates that more than 128 million pieces of space debris exist between a millimeter and a centimeter.[70]

The distribution of these tracked objects, as well as the distribution of their overall mass, is critical for fully understanding the context of the space debris problem. This is true because, just like operational satellites, the rest of the SSN's tracked space objects are not distributed equally throughout space. Most of this debris is found in incredibly important orbits, particularly in LEO between 600 and 1,500 kilometers and in GEO.[71] More than 60% of these objects are concentrated in LEO, with GEO making up the second most populous orbit.[72] The same can be said for the overall mass of these tracked space objects, but slightly less concentrated in LEO. The total mass of tracked objects in space is in excess of 8,000 metric tons,[73] of which well over 95% is made up of payloads and discarded rocket bodies.[74] Fragments and mission related debris only make up about 2% each.[75] The highest overall mass is concentrated in LEO, but GEO is not far behind, since payloads there are much older, some weighing as much as six tons.[76]

In short, while there are vast numbers of objects orbiting Earth, well over 85% of what can be tracked is space debris. Further, this debris is most concentrated in the important LEO and GEO regions, whether measured in quantity or mass.

C. Dangers of Space Debris

The statistics presented above would be unremarkable but for the fact that space debris poses significant dangers to both global space operations and the environment itself. For example, space debris can threaten the viability of both manned and unmanned space operations. Excess debris can also over-pollute valuable Earth orbits or even threaten the surface of the Earth with falling debris that can contain chemical or nuclear hazards.

1. Manned and Unmanned Space Operations

It is clear that space debris, especially small, untrackable pieces, can be dangerous to both manned and unmanned space operations. Satellite owners can utilize physical barriers to shield against debris smaller than one centimeter and, therefore, this debris generally only poses the risk of degradation or partial functional damage.[77] However, space debris over one centimeter cannot be effectively shielded against, and therefore poses a risk of severe or even catastrophic damage.[78]

Satellites routinely face unexplained anomalies, often only attributable to collisions with very small pieces of space debris. However, the first explainable collision between catalogued objects occurred in July 1996, when a legacy fragment from an exploded ESA Arianne rocket body collided with a 50-kg French microsatellite called 'Cerise' while orbiting at approximately 670 kilometers in altitude.[79] This collision destroyed the six meter gravity boom which stabilized the satellite.[80] Fortuitously, it cleanly severed the boom and created only a single piece of trackable debris, the broken portion of the boom itself.[81] While the SSN warns satellite operators when its modeling software predicts such close encounters, known as "conjunction events," satellite operators may be unwilling or unable to navigate their satellites away from the space debris.

When it comes to manned space operations, the risks posed by space debris rapidly become more serious. For example, with regard to the crewed U.S. Space Shuttle, these risks prompted NASA to commission a "Space Shuttle Meteoroid and Debris Damage Team."[82] Post-mission analysis of the windows of the space shuttle revealed that pits were caused by debris impacts in orbit on every single mission,[83] leading to the replacement of 70 Shuttle windows between 1981 and 1998.[84] After considering the impact of debris on the Space Shuttle and using statistical modeling, NASA concluded that a 10-day Shuttle mission at 400 kilometers would, on average, result in more than 800 collisions with debris between .04 and .1 millimeter in size.[85] Notably, collision with a piece of debris of only 5 millimeters was likely to penetrate the crew cabin.[86] Of course,

the most permanent, and therefore risky, human presence in outer space is that of the International Space Station (ISS), which continuously houses astronauts from various contributing nations and maintains an orbital altitude of roughly 400 kilometers.[87] Conjunction with a piece of space debris, especially one in excess of 10 centimeters, could easily result in the loss of human life aboard the ISS. To manage this risk, the ISS has been forced to conduct 25 relocations, or "debris avoidance maneuvers," since 1999.[88]

2. Environmental Contamination

In addition to endangering manned and unmanned space operations, one of the most discussed risks of space debris is what has become known as the Kessler Syndrome, or the possibility for several major conjunction events to create a continuing knock-on effect that renders certain orbits contaminated and unfit for future space operations. This effect is based on Donald Kessler's original description of the risk of a rapidly forming "debris belt."[89] The problem with such a runaway cascade is that the resulting slew of space debris fragments may stay in orbit for incredibly long periods of time, depending on their altitude, surface area, mass, density, and a number of other atmospheric characteristics and influences.[90] For reference, a one kilogram CubeSat in a circular orbit at 600 kilometers will likely remain in space for approximately 32 years.[91] However, the orbital duration exponentially increases as orbital altitude increases, so much so that the IADC describes the average atmospheric drag-induced orbital lifetime for a typical spacecraft above 1,000 kilometers as "quasi-eternal."[92]

In addition to long-term environmental contamination in space, space debris can also impact the surface of the Earth, since debris in LEO will eventually re-enter the Earth's atmosphere. If the space object is large enough to survive reentry, it can pose a falling risk to humans on the ground.[93] Further, any chemical or nuclear material that survives re-entry can pose serious environmental dangers to the atmosphere or the surface of the Earth. One notable example of such danger occurred in 1978, when the Soviet satellite 'Cosmos 954,' powered by 50 kilograms of enriched uranium, crashed into northwestern Canada, sprinkling radioactive material across more than 100,000 square kilometers.[94]

D. Increase in Space Debris over Time

An even cursory glance at NASA's data sets reveals the total quantity and mass of catalogued space objects has been steadily increasing since the dawn of the space age. Between 1970 and 2018, the overall quantity of catalogued objects in space increased from approximately 2,800 to roughly 18,700, a growth

of 567%.[95] Staggeringly, the overall mass of these objects during this same time increased from nearly 375 metric tons to approximately 7,700 metric tons, an increase of 1,953%.[96] The explanations for these dramatic and continued increases are broad, but can be partially explained by the intentional and accidental fragmentation of satellites, as well as the increase in space-faring nations and commercial space operations.

1. Fengyun-1C ASAT Test (2007)

One of the most dramatic contributions to the quantity of catalogued objects, and to fragmentation debris generally, is the intentional kinetic destruction of satellites from the military testing of ASAT capabilities. Four different countries have conducted such destructive ASAT tests across a timespan of over 50 years, as recently as March 2019.[97]

By far the most prolific debris-creating ASAT test was China's destruction of its defunct Fengyun-1C weather satellite in 2007. This polar-orbiting satellite was destroyed by a direct ascent ASAT at an altitude of approximately 865 kilometers,[98] creating more than 3,312 pieces of tracked debris.[99] It is estimated that an additional 32,000 pieces of untracked debris were also created.[100] A few years after the test, the debris field was scattered between 175 and 3,600 kilometers in altitude, in total representing 22% of all catalogued objects in LEO in 2010.[101] Debris from this test has caused the defensive movement of other satellites and even the ISS.[102] It is predicted that only approximately 21% of the debris from this ASAT test will decay and fall out of orbit by the year 2107.[103] In other words, roughly 79% of the entire debris field may still be orbiting the Earth a full century after the ASAT test was conducted.[104]

2. Cosmos 2251/Iridium 33 Collision (2009)

While intentional fragmentation events like ASATs can cause large debris fields, so can accidental collisions. The largest such accidental collision was the result of a defunct Russian military communications satellite, Cosmos 2251, and an operational U.S. commercial communications satellite, Iridium 33, colliding over Siberia in 2009 at approximately 790 kilometers in altitude.[105] This event was the first recorded instance of two satellites accidentally colliding with one another in space.[106] Cosmos 2251 had an impressive mass of 900 kilograms, while Iridium 33 was smaller, but still a sizeable satellite, at 556 kilograms.[107] The collision caused Cosmos 2251 to fragment into 1,668 catalogued pieces of debris over 10 centimeters, while Iridium 33 broke up into 628 such pieces.[108] Thousands of additional pieces of debris less than 10 centimeters were also created.[109] The collision scattered

debris across varying altitudes between 200 and 1,700 kilometers,[110] but was concentrated in the critically important LEO altitudes around 800 kilometers.[111] Some of this debris has even threatened the ISS, requiring it to perform a debris avoidance maneuver in 2015.[112] Scientific modeling predicts that a significant proportion of Iridium 33's fragments will remain in orbit for more than 100 years, while a significant amount of Cosmos 2251's debris will be in orbit for at least 25-50 years.[113] Behind the Chinese Fengyun-1C ASAT test, Cosmos 2251 and Iridium 33 are individually the number two and number four largest debris-creating fragmentation events in history, respectively.[114]

3. Indian ASAT Test (2019)

Another important debris-creating ASAT test occurred in March 2019, when India intentionally destroyed its own 740-kilogram Microsat-r satellite at an altitude of approximately 285 kilometers.[115] This satellite had been launched by India just two months prior to carrying out the ASAT test.[116] The resulting fragmentation created, as of May 2019, at least 84 pieces of trackable debris larger than 10 centimeters, in various orbits ranging from 200 all the way up to 2,250 kilometers in altitude, plus many additional pieces of smaller, untrackable fragments.[117] Importantly, this debris field threatens the ISS, as approximately 79% of the created debris orbits in altitudes above it.[118]

While this debris-creating episode is nowhere near the magnitude of the Chinese Fengyun-1C test, it is worth highlighting simply because it demonstrates that, even in 2019, States are still willing to knowingly and intentionally create space debris in vital Earth orbits.[119]

4. Space-Faring Nations and Commercial Space Activities

In addition to the increase in space debris from dramatic fragmentation events, the total volume and mass of debris in the space environment is also increasing simply because there are more space participants than ever before, whether calculated in terms of space-faring nations or commercial activities. In the 1950s, only the United States and the Soviet Union were active in space. Through the 1960s, another six countries joined them.[120] By 2011, that number had grown to more than 50.[121] As of mid-2020, there are at least 82 countries which have government or commercial satellites in orbit, in addition to dozens more intergovernmental entities,[122] and more are joining these ranks all the time.

Further, the global space economy has undergone incredible growth in the last several decades. In 2009, it was a U.S. $150-165 billion industry.[123] By the end of 2016, it was estimated to be worth roughly U.S. $345 billion,[124] driven largely by the meteoric growth of commercial space launches when compared against government launches. For example, SpaceX, a private U.S. company, has dramatically increased its role in launch services, conducting 17 of the 22 FAA-approved orbital launches in the U.S. in 2017.[125] New commercial companies are also revolutionizing the way space is accessed and exploited, using lean, agile startups to develop smaller (in both surface area and mass), cheaper, and more numerous satellite constellations, a shift in the space industry known as "NewSpace."[126] No longer simply supporting government operations, commercial entities are themselves becoming "key protagonists" in space.[127]

This exciting and ambitious new commercial approach to space is not likely to slow down anytime soon. In fact, it is only expected to increase. The market has recently enjoyed annual average growth of 6-8% and is projected to be worth between U.S. $1-2.7 trillion by the 2040s.[128] Companies are also going public with ambitious plans for massive new satellite constellations, designed to deliver commercial services to every corner of the globe. For example, OneWeb, a communications company, has launched the first 74 satellites in its anticipated 650-satellite constellation in LEO to provide global broadband internet coverage, with plans to potentially scale up to either 900 or 1,980 total satellites.[129] Similarly, Amazon has announced "Project Kuiper," its plan to develop a 3,236-satellite broadband internet constellation across three LEO altitudes.[130] Dwarfing all other projects, SpaceX's global broadband internet plan, called "Starlink," has already received FCC approval for 12,000 satellites to be arranged in dozens of rings in multiple LEO orbits, with an eventual goal of scaling upwards to as many as 42,000 satellites.[131] These commercial plans represent a marked paradigm shift in outer space, given the fact that there were only 994 total active satellites in Earth orbit in 2012.[132]

Facilitating this increase in new State and commercial activity in space is the fact that the costs associated with gaining access to space have been rapidly decreasing.[133] These decreases are partially due to the development of new space launch technology, like SpaceX's Falcon and Falcon Heavy rockets, but also because record numbers of smaller payloads are being combined into single launches, sharing the costs among many operators. For example, in 2017 India launched 104 satellites on a single mission, nearly tripling the previous world record of 37 set by Russia in 2014.[134]

E. Conclusion

Space debris can be classified as either mission-related debris, fragmentation particles, microparticulates, jettisoned rocket bodies, or derelict payloads. While the SSN and other networks take great efforts to track and catalogue this debris, there are limits to what can be monitored, depending on the object's orbital altitude and size.[135] Overall, space debris has been on a steady upward trend, both in mass and quantity, ever since the first days of human activities in space and shows no sign of slowing down. Worryingly, the most dramatic increases in space debris have occurred due to intentional fragmentation events, specifically kinetic ASAT tests, which are continuing to occur. Other major fragmentation events have resulted from collisions or simply the on-orbit fragmentation of derelict payloads and rocket bodies. Apart from fragmentation events, space is simply becoming more congested as more and more States and commercial entities exploit the cheap access which advances in technology have provided. Not only will this increased space activity generate even more debris, but the congestion itself will increase the threat posed by already existing debris. The overall quantity and mass of the debris from all of these sources are not uniformly distributed across space; rather, they are concentrated in the most heavily used orbits, primarily in LEO and GEO, and therefore pose a danger to both manned and unmanned space operations as well as to the space environment.

II. Space Debris Mitigation Efforts and Failure

The space debris problem described in Part I began to catch the eye of scientists, governments and intergovernmental entities in the 1980s and early 1990s.[136] Eventually, the U.N. added it as a recurring item on COPUOS' STSC agenda, beginning in 1994.[137] However, no hard law has been adopted at the international level to address this problem. Instead, various States and intergovernmental organizations began devising and applying their own strategies to mitigate the creation of additional space debris from future space activities and to apply these strategies to space operators through national laws and space licensing requirements. Eventually, in the 2000s, two major international mitigation guidelines were developed on a voluntary, non-binding basis and gained broad support, namely those of the IADC and the COPUOS STSC. While an encouraging first step, these voluntary, soft law guidelines appear to be the preferred method of regulating debris on the international stage, as opposed to any binding legal obligations.[138] It is the contention of this article that these mitigation efforts have failed to adequately address the escalating problem of space debris.

A. Early National and International Space Debris Mitigation Efforts

The earliest national efforts towards a comprehensive space debris mitigation guideline began in the United States in the mid-1990s with NASA, specifically NASA's "Guidelines and Assessment Procedures for Limiting Orbital Debris" in 1995.[139] This guideline implemented NASA's earlier 1993 announcement of Management Instruction (NMI) 1700.8, which had simply ordered each program to conduct a formal assessment of their potential to create debris.[140] The new, more specific guidelines further required all new NASA programs to conduct orbital debris assessments within the program's development phases and to generate debris assessment reports for review and concurrence.[141]

While NASA was undertaking these efforts, two influential U.S. organizations were also analyzing the space debris problem, namely, the U.S. National Research Council and the National Science and Technology Council. Debris reports from each organization were released in 1995[142] and were influential in leading to the first iteration of a coherent national U.S. debris mitigation strategy[143] in 1997, called the U.S. Orbital Debris Mitigation Standard Practices (ODMSP).[144] The ODMSP contained four basic, but now standard, mitigation strategies: control debris released during normal operations, minimize accidental explosions, minimize opportunities for collisions, and dispose of payloads and launch vehicle components post-mission.[145]

Very soon after NASA developed its mitigation guidelines in 1995, the space agencies of other countries began to follow suit. In 1996, the National Space Agency of Japan (NASDA) promulgated its own mitigation standards,[146] which contained many of the same objectives as the NASA standard.[147] In 1999, France's Centre National d'Études Spatiales (CNES) published its own debris mitigation standards,[148] which later served as a model for a European-wide standard.[149] Only one year after that, Russia's Roscosmos also developed its own standards.[150] Similar criteria were later adopted in China, Canada, and a host of other countries.[151] To ensure compliance, most States incorporated these standards into national law or enforced their national guidelines through their licensing procedures.[152]

While each State was determining the appropriate level of debris mitigation standards to impose upon its nationals, international and intergovernmental bodies were hoping to standardize debris mitigation efforts across space-faring nations. As far back as 1994, the International Law Association (ILA) developed its Draft Convention on Space Debris,[153] with a major focus of addressing the debris problem in tandem with liability and responsibility concerns.[154] Despite

substantive contributions to the development of mitigation standards, the ILA Convention failed to develop into a legally binding international instrument.[155]

The ESA, a major intergovernmental space body, was also looking to standardize mitigation efforts. It promulgated a draft European Space Debris Safety and Mitigation Standard as well as a Space Debris Handbook in 2000. Together, these two documents regulated the implementation concepts and technical recommendations for debris mitigation and collision risk reduction for all space projects developed or controlled by ESA.[156] Thereafter, ESA and the major national space agencies of Europe concluded the European Code of Conduct for Space Debris Mitigation in 2004.[157] While widely subscribed to by European space-faring nations, the Code of Conduct has been criticized as imprecise and difficult to enforce, mainly due to its voluntary nature.[158] More recent European attempts to coordinate the responsible and sustainable use of space have been conducted through the EU's diplomatic effort since 2012 to develop a wide-ranging, but non-binding and voluntary, Draft International Code of Conduct for Space Activities.[159] Notably for space debris mitigation, any potential adherent to this draft code would "resolve" to "refrain" from the intentional destruction of space objects, presumably a notional agreement not to conduct ASAT tests.[160] However, the draft code's future is uncertain since many States have raised various objections during its negotiation, while some others have simply refused to participate.[161]

Another international forum for debris mitigation standards emerged through the International Organization for Standardization (ISO), which is an independent, non-governmental membership organization aimed at the voluntary streamlining of international standards for its more than 160 member states.[162] In 2010, the ISO's body of international industry experts developed Standard 24113, "Space Systems – Space Debris Mitigation Requirements." This effort differed from some of the loftier guidelines which proved difficult to implement; instead Standard 24113 helped to normalize the more technical aspects of debris mitigation in outer space, enabling the application of somewhat streamlined design principles.[163] Standard 24113 was updated in 2011 and has been adopted by both the ESA and the European Cooperation for Space Standardization (ECSS).[164]

The International Telecommunication Union (ITU) also provides some guidance when it comes to space debris mitigation, specifically in GEO. The ITU is a specialized U.N. agency responsible for the allocation of global radio spectrum and satellite orbits.[165] While founded on a multilateral treaty, the ITU also provides guidance in the form of recommendations. In 2010, it promulgated Recommendation ITU-R S.1003-2, "Environmental Protection of the Geostationary-Satellite Orbit," which provides operational guidance for satellites in GEO, with an eye

towards protecting the GEO region and reducing space debris.[166] Specifically, it encourages space operators to minimize debris creation in GEO and GEO transfer orbits, as well as to boost their satellites into a graveyard orbit of not less than 200 kilometers above GEO at their end of life.[167] Like the other international efforts towards debris mitigation noted above, ITU-R S.1003-2 is only a recommendation to the ITU member states and is not legally binding on member States.[168]

B. IADC Space Debris Mitigation Efforts

The focus on debris mitigation by the various nations, their national space agencies, and international and intergovernmental organizations discussed above eventually coalesced around the IADC in the early 2000s. The IADC itself was founded by NASA, ESA, Roscosmos, and Japan in 1993[169] as an "international forum of governmental bodies for the coordination of activities related to the issues of man-made and natural debris in space."[170] Its primary purpose is to provide opportunities for cooperation and the exchange of information related to space debris research activities amongst its members, as well as to identify debris mitigation strategies.[171] It has since grown to include 13 member agencies, including most of the world's major national space agencies.[172] In 2002, the four founding members plus seven newer members, notably including China's National Space Administration (CNSA) as well as the national space agencies of India, France, Italy, Germany, and the UK, developed a comprehensive set of guidelines called the IADC Space Debris Mitigation Guidelines (hereinafter "IADC Guidelines"), which were agreed to by consensus.[173] These guidelines were updated in 2007 and have become remarkably successful, despite only being voluntary.[174] In fact, they have been described as the "basis against which the world community is measuring success" and a "standard for the responsible space operator."[175] As such, most States and intergovernmental space organizations, including the U.S., the UK, and ESA, maintain domestic standards which are compliant with the IADC Guidelines.[176]

The updated 2007 IADC Guidelines describe the existing practices which have been identified and evaluated by various States to aid in limiting the generation of debris in space.[177] They particularly focus on (1) limiting debris released during normal operations, (2) minimizing the potential for on-orbit breakups, (3) post-mission disposal, and (4) preventing on-orbit collisions.[178] They are designed to apply to mission planning and the design and operation, including the launch, mission, and disposal, of all spacecraft and stages intended to be operated in Earth orbit.[179] Importantly, the IADC Guidelines were the first to define space debris as "all man-made objects including fragments and elements thereof, in Earth orbit or re-entering the atmosphere, that are non-functional."[180]

It establishes LEO and GEO ± 200 kilometers and ± 15 degrees inclination as "protected regions" of space, worthy of unique attention for debris mitigation efforts.[181] The IADC Guidelines also encourage the creation of a Space Debris Mitigation Plan for every project or program in order to manage the implementation of its mitigation measures.[182]

Regarding limiting debris during normal operations, the IADC Guidelines recommend designing spacecraft and orbital stages such that no debris is intentionally released during normal operations, or if necessary, that it is limited as much as possible.[183] Further, the Guidelines recommend conducting an assessment to ensure that the risk from any released debris to other spacecraft and the environment itself is "acceptably low."[184]

In order to minimize on-orbit breakups, the IADC Guidelines recommend depleting any stored, on-board energy sources, such as batteries, propellants, or flywheels.[185] It also states that "intentional destructions, which will generate long-lived orbital debris, should not be planned or conducted."[186]

The IADC Guidelines also recommend post-mission disposal of GEO spacecraft well above the highest edge of the protected region, at an altitude of not less than 235 additional kilometers.[187] For spacecraft or orbital stages terminating in orbits which pass through LEO, the IADC Guidelines recommend that, presuming they are not being directly de-orbited, the post-mission orbital lifetime should be kept under 25 years.[188] In other words, at their end-of-life, spacecraft should be physically lowered to at least an altitude which will allow for natural decay due to atmospheric drag and other space forces within a 25-year window.

Finally, the IADC Guidelines recommend designing spacecraft to limit the consequences of collision with small debris, usually accomplished via shielding, and to maneuver spacecraft or coordinate launch windows as necessary to avoid other collisions.[189]

Despite their wide acceptance as a common baseline for debris mitigation efforts, the IADC Guidelines have been criticized for failing to give technical or functional advice regarding their practical implementation.[190] However, this complaint is somewhat lessened by the IADC's issuance of a supplementary support document to the Guidelines which provides the purpose behind and specific practices for each recommendation.[191]

C. United Nations Space Debris Mitigation Efforts

At the same time that the IADC was working on its Guidelines, the U.N. was also studying the space debris problem, with an eye towards standardizing debris mitigation efforts globally. In 1999, the STSC of COPUOS released a comprehensive report which concluded that debris mitigation efforts were "a prudent step towards preserving space for future generations."[192] Putting this conclusion into action, the STSC then sought to build upon the success of the IADC Guidelines by pushing for broader, global consensus for debris mitigation within the U.N. This goal was eventually achieved in early 2007 in the form of the COPUOS Space Debris Mitigation Guidelines (hereinafter "COPUOS Guidelines).[193] The entire United Nations General Assembly (UNGA) later endorsed these voluntary guidelines and further invited U.N. member-States to implement them through their own national mechanisms.[194]

The COPUOS guidelines are greatly influenced by and are nearly identical to the IADC Guidelines, which preceded them by almost five years.[195] As such, the COPUOS Guidelines adopt the IADC definition of "space debris" and similarly discuss limiting debris from normal operations, the passivation of on-board potential energy or power sources, collision avoidance, preferred end-of-life orbits, and avoiding intentional destruction.[196]

While the two sets of Guidelines are very similar, there are several important discrepancies, primarily because the IADC Guidelines are more detailed in nature.[197] For example, the IADC Guidelines discuss a specific altitude and formula for GEO end-of-life "graveyard" movements, while the COPUOS Guidelines merely recommend non-interference with GEO after the termination of operations.[198] Similarly, in relation to post-mission orbits affecting LEO, the IADC Guidelines expressly endorse a 25-year maximum orbital lifetime, while the COPUOS Guidelines refrain from suggesting any specific maximum orbital lifetime.[199] Unlike the IADC Guidelines, the COPUOS Guidelines affirmatively declare that exceptions to them may be justified.[200] In that sense, they appear more technically than legally oriented, especially since COPUOS' Legal Subcommittee played no part in their development.[201] Such differences between the IADC and COPUOS Guidelines may be explained by the concessions necessary to gather consensus in the larger and more political UN setting.[202] However, despite any required concessions, endorsement by the UNGA means that the COPUOS Guidelines enjoy appreciably broad international support.

In the more than 13 years since the promulgation of the COPUOS Guidelines, no further updates have been made, despite the dramatic increases observed in space debris. Instead, the "Long-Term Sustainability of Space Activities" was added as a COPUOS agenda item in 2010, resulting in the creation of a working group in the STSC focusing, in part, on space debris as an aspect of space sustainability.[203] In 2018, this agenda item eventually resulted in COPUOS agreeing by consensus to a set of "Guidelines for the Long-Term Sustainability of Outer Space Activities."[204] However, these guidelines contain little in the way of debris mitigation, other than to suggest wider compliance with the 2007 COPUOS Guidelines.

D. Failure of Space Debris Mitigation Efforts/Need for Active Debris Removal

The drafting and widespread acceptance of the IADC and COPUOS Guidelines, as well as other national guidelines and technical standards, are significant first steps towards slowing the growth of space debris. They have especially aided in reducing debris creation in certain contexts, such as the release of mission-related debris.[205] However, these two primary international mitigation efforts have significant, inherent limitations, some of which lead to a lack of compliance by space operators. Ultimately, both have failed to halt the continued increase in debris, whether measured by mass or quantity. Leading experts and space agencies now agree that mitigation efforts alone are insufficient to tackle the debris problem going forward; active debris removal must be implemented in conjunction with mitigation efforts.

1. Limitations of the Guidelines

While the IADC and COPUOS guidelines are, no doubt, an integral part of the solution for tackling the current debris problem, it is also important to note several structural limitations contained within them which have severely hampered their efficacy.

The most obvious and notable limitation of these two leading international guidelines is that they are entirely voluntary and non-binding.[206] The IADC Guidelines simply "encourage" compliance, while the COPUOS Guidelines state outright that they are "not legally binding under international law."[207] Because of this, even States which adhere to the guidelines retain the freedom to abide by them or disregard them.[208] Further, the guidelines offer no direct incentives for compliance[209] and are only applicable to private or commercial entities to the extent that national legislation requires compliance and thereafter actually enforces the guidelines.[210] Many compare this soft law regime to a "tragedy of

the commons," or a situation in which actors continue to detrimentally exploit the pool of resources out of fear that complying with restrictive regulations will put them at a disadvantage as compared to others.[211] One commentator summed up this shortcoming succinctly by stating that:

> "because guidelines are unenforceable by nature, orbital debris mitigation rests predominantly on the amount of goodwill that states are willing to extend in voluntarily restricting themselves and their national operators from creating debris. Here the major space powers in this debate will likely continue to privilege their freedom of action in their activities over submitting to binding restrictions from international organisations, to ensure the security of their assets in orbit."[212]

Another significant structural limitation of the IADC and COPUOS Guidelines is that they are, by the very nature of the space environment, prospective standards as opposed to retrospective fixes. They are designed to be forward-looking and are meant to be applied to future mission-planning and "newly designed" spacecraft and orbital stages.[213] In contrast, they are only designed to be applied to already existing spacecraft "if possible" or "to the greatest extent feasible," which is often not at all.[214] Further, legacy orbiting satellites and rocket bodies designed, planned, and launched in the 1950s or 1960s are almost certainly unable to be redesigned, modified, passivated, or moved into a graveyard orbit today.[215] Instead, they are largely defunct and uncontrolled. As the ultimate example, neither the IADC nor COPUOS Guidelines can offer any feasible mitigation action to take with regard to the oldest currently orbiting satellite, the U.S. Vanguard 1, which was launched in 1958 but ceased transmitting in 1964.[216] Further, these guidelines do nothing to address the enormous amount of other forms of existing space debris, such as uncontrolled rocket bodies or small pieces of debris from fragmentation events. This is a very significant shortcoming of the guidelines since, as noted before, all forms of space debris together constitute roughly 90-95% of the catalogued objects in space.[217] The best these mitigation guidelines can offer are strategies to minimize the risks of creating more debris in the future, while essentially ignoring the debris problem as it currently exists.

Additionally, neither the IADC nor COPUOS Guidelines effectively deter the intentional destruction of on-orbit space objects through ASAT tests. Instead, they merely encourage States to avoid the intentional destruction of spacecraft and orbital stages if it will "generate long-lived orbital debris."[218] However, despite both guidelines using terms like "long-lived," "long-term presence," "over the longer term," "long term interference," etc, neither set of guidelines defines what duration

is envisioned by use of the word "long." Presumably, since the IADC Guidelines set 25 years as an acceptable post-mission orbital lifetime for payloads in LEO (described therein as "reasonable and appropriate"),[219] it is fair to conclude that anything less than a 25-year orbital lifetime should not be considered "long-term." If that is the case, then ASAT tests which generate, for example, 20-year debris fields could arguably be justified as entirely consistent with the IADC Guidelines. Further, rather than any sort of blanket restriction on ASAT tests, both guidelines seem to normalize the international acceptance of such tests by stating that, "when necessary," they "should be conducted at sufficiently low altitudes such that orbital fragments are short-lived."[220] Similar to their treatment of the phrase "long-term," neither guideline elaborates on exactly what "necessary," "sufficiently low," or "short-lived" means. Given the ASAT tests discussed in Part I(D)(1) and (3), *supra*, the IADC and COPUOS Guidelines have clearly not deterred States from conducting ASAT tests which create "long-term" debris by any standard.

Additionally, the IADC and COPUOS Guidelines fail to consider or provide any sort of tailored guidance for wartime or national security related activities.[221] While peacetime military activities in space are beginning to comprise a smaller percentage of all space operations, they are still significant,[222] especially since conventional, direct-ascent ASAT weaponry does not exist in the commercial sector. Wartime military operations, without the restraint imposed by focused guidelines, could be devastating to the orbital environment. Further, national security-related activities in space are largely carried out by government actors, which are subject to internal policy guidelines rather than the traditional, national licensing mechanisms most often used to implement the IADC and COPUOS Guidelines.[223] As such, these government activities in space are likely to favor national security and freedom of operation over strict adherence to mitigation guidelines.[224]

Finally, while the IADC and COPUOS Guidelines discuss de-orbiting and re-orbiting measures for protecting the LEO and GEO regions, there is no discussion of end-of-life mitigation measures related to MEO at all. In order to preserve all Earth orbits, end-of-life issues related to the numerous GNSS constellations should also be included in these guidelines.[225]

2. Problems with Compliance

In addition to the structural limitations discussed above, there are also notable problems with IADC and COPUOS Guideline compliance. This is true despite the fact that these documents were derived through consensus in both the IADC and the U.N., encompassing all of the leading space-faring States,[226] and that they have been widely implemented into national licensing mechanisms. Nevertheless,

while certain aspects of the Guidelines enjoy broad uniformity, such as spacecraft design or passivation measures, compliance remains an acute problem when it comes to end-of-life operations or the intentional creation of debris.

In the protected LEO region, for example, compliance with the IADC's 25-year de-orbit guideline is mediocre at best. In 2017, the most recent year for ESA-compiled payload compliance data for LEO at the time of writing, only approximately 55% of payloads in LEO at their end of life were compliant with the 25-year rule.[227] Over 40% of all payloads in this region made no attempt whatsoever to clear LEO at their end of life,[228] comprising almost 60% of total end-of-life payload mass.[229] In one study, observing LEO end-of-life de-orbiting of payloads between 2000 and 2013, it was concluded that only approximately half of all spacecraft even possessed orbit control capability.[230] Of those, just 27% performed end-of-life maneuvers, representing a mere 12% of the total spacecraft population in LEO.[231] Between 2000 and 2013, compliance with the 25-year de-orbit rule in LEO for payloads averaged 59%,[232] but has dipped as low as 20% in a single year, as it did as recently as 2008.[233] If naturally decaying payloads are excluded from this equation, fewer than 20% were successfully cleared from LEO at their end-of-life in 2017, while almost 80% never even made an attempt to clear it.[234] When it comes to the mass of these same satellites, the true scope of non-compliance is revealed. In 2016, one of the worst years on record since 1990, less than 30% of the total mass of all end-of-life LEO payloads complied with the 25-year rule.[235] Rocket bodies, as opposed to payloads, recently fare slightly better in LEO, with nearly 80% complying with the 25-year IADC rule in 2018.[236] However, compliance rates for rocket bodies in LEO between 2000 and 2013 are estimated at 60% overall, virtually the same as payloads.[237] This figure should increase in the future as the controlled re-entry of rocket bodies after launch is beginning to increase.[238] To painfully sum up LEO compliance with the guidelines, the IADC's Chairperson briefed the STSC of COPUOS in 2018 to the effect that "the current implementation level is considered insufficient and no apparent trend towards a better implementation is observed."[239]

In GEO, the situation is slightly better. In 2018, more than 85% of the 16 disposed GEO satellites cleared the protected region.[240] This accounted for nearly 90% of the combined mass of the disposed satellites for 2018.[241] While this sounds promising, the compliance data can vary significantly depending on the year. In 2008, only seven of the 12 retired satellites were re-orbited properly,[242] and in 2015, a full 13 years after the IADC Guidelines were originally drafted, only five of 12 satellites in GEO were properly disposed of at their end-of-life.[243] Despite these low-performing periods, the IADC stated in 2018 that it has observed "a trend towards satisfactory levels" of GEO re-orbiting compliance in recent years.[244]

When it comes to the intentional creation of debris, States have on occasion radically departed from the two major guidelines, resulting in disastrous consequences. The most flagrant example of noncompliance, which resulted in the worst fragmentation event in history, was that of China's intentional destruction of Fengyun-1C in 2007, discussed *supra* in Part I(D)(1). Interestingly, prior to this event China had seemingly engaged in debris mitigation efforts on both the domestic and international fronts: it was a founding member of the IADC; actively participated in the drafting of the 2002 IADC Guidelines; released its own domestic Working Plan for Space Debris in 2003 and Requirements for Space Debris Mitigation in 2005; and signed the updated 2007 IADC Guidelines.[245] Yet, China still broke with the IADC Guidelines to intentionally destroy its satellite at an altitude that was certain to create a significant and long-lasting debris field, violating the spirit of the mitigation guidelines. China is not alone in this regard. The United States destroyed a satellite with a direct-ascent ASAT as recently as 2008, as did India in 2019.[246] While these tests varied from China's 2007 test in both altitude and the resultant debris field,[247] all have arguably softened both the IADC and COPUOS Guidelines' provisions that such intentional fragmentations "should be avoided" unless "necessary," and even then, only at "sufficiently low altitudes."[248] It is clear that national security concerns can lead to noncompliance with the IADC and COPUOS Guidelines. However, even if only an infrequent event, just a single act of noncompliance with the intentional destruction provisions has the capacity to cause significant, long-term implications for the space debris problem.

3. Failure to Reduce Debris

More telling than the structural limitations or compliance problems with the Guidelines is the clear failure of focused mitigation efforts since 2002 to halt the growth of debris. In essence, the more than 15-year trend in space debris growth after the implementation of these Guidelines speaks for itself.

From 2002 through 2018, the total catalogued mass of space objects has increased from roughly 4,750 to about 7,700 metric tons.[249] The quantity has experienced similar growth, from approximately 11,500 catalogued objects to almost 19,000.[250] Importantly, as of mid-2020, only about 3,000 of these catalogued objects are actually functioning satellites; the rest are considered space debris.[251] Mitigation efforts have not only failed to reduce the total amount and mass of space debris, they have failed to appreciably slow its growth rate. While there had been a slight trend of reduction in specifically fragmentation debris between 2011 and 2016, any derived benefit was erased many times over by both intentional and accidental fragmentation events.[252] As has been stated, "years of successful mitigation can be negated by a single large event."[253]

This growth trend in debris is expected to continue into the future in LEO even if mitigation guidelines related to end-of life disposal are complied with at a rate of 90%.[254] It will similarly continue to grow even assuming no future explosive fragmentation events occurred at all[255] or even if all new space launches were ceased entirely.[256] These are arguably unrealistic expectations given recent data. It is clear that mitigation alone does not offer a viable solution to the space debris problem.[257] Instead, research has shown that mitigation efforts must be combined with active debris removal in order to stabilize the growth of debris in LEO.[258]

4. Consensus of Space Experts and Agencies

While the data above is clear, it is also worth briefly noting the voices of major space experts and agencies on this issue. The majority of these experts and agencies are in clear agreement that mitigation efforts alone have proven themselves insufficient and that ADR must be actively pursued.

As far back as 2006, Jer Chyi Liou, NASA's current Chief Scientist for Orbital Debris, argued using statistical modelling that LEO's debris population was unstable and that growth would continue even with widespread implementation of mitigation measures.[259] He and his co-author concluded that ADR is the *only* solution.[260] Thereafter, the IADC pegged this issue as an official action item and similarly concluded in 2013 that, even assuming 90% compliance with commonly adopted mitigation measures, the LEO debris population will continue to grow.[261] Notably, the statistical modeling programs of the national space agencies of Italy, India, Japan, the U.S. and the U.K., as well as ESA, all unanimously supported this conclusion.[262] Such research ultimately led the U.S. to formally declare that its ODMSP has been rendered "inadequate to control the growth of orbital debris."[263]

By 2017, the ESA-sponsored 7th European Conference on Space Debris, comprising hundreds of space industry, academic, and policy experts, also concluded that the existing space debris mitigation rules are insufficient.[264] Unsurprisingly, Holger Krag, the head of ESA's Space Debris Office at the European Space Operations Center, which represents the interests of 22 member countries, also shares that opinion. He has long concluded that even strict implementation of the current mitigation measures will not stop future debris growth and that "the only possible way to achieve stability while continuing space activities is to perform ADR."[265]

E. Conclusion

After taking note of the growing threat of space debris in the 1980s, NASA and other national space agencies began to consider ways of mitigating the creation of new debris. Eventually major international efforts took place to develop comprehensive voluntary guidelines to rein in new debris creation. The first of these was promulgated by the IADC in 2002 and was later modified and adopted by COPUOS and the UNGA in 2007, eventually gaining widespread international support. Other agencies, like the ITU and the ISO, also contributed to the standardization of debris mitigation efforts. However, these mitigation efforts have failed to control the space debris problem, both due to various structural limitations within the guidelines themselves and due to a failure of space-faring nations and their citizens to faithfully implement them. Even the IADC itself bemoans the collective rate of compliance. Ultimately, the space debris population has continued to see significant increases, most notably in LEO. Space agencies and experts around the world are now in virtual unanimous agreement that mitigation efforts alone are insufficient and that ADR is absolutely necessary to stabilize vital Earth orbits. However, many challenges must be overcome before an effective ADR regime can be established to tackle the debris problem.

III. Active Debris Removal and Its Current Challenges

In the face of the previously described debris problem and the failure of the various mitigation efforts made by the majority of space-faring nations to bring it under effective control over the last 30 years, active debris removal has now become a necessity. However, there are significant challenges complicating the successful implementation of ADR. Part III briefly overviews several of the most promising ADR technologies, whether based in space or conducted from the surface of the Earth. Thereafter, it analyzes the most pressing legal and policy challenges complicating the successful implementation of ADR.

A. Description of Active Debris Removal Technologies

Currently, while there are not yet fully operational ADR technologies,[266] there are a plethora of proposed methods to remove space debris from Earth orbit.[267] Only a few have been physically tested *in situ*; much ADR technology remains conceptual and none is sufficiently advanced to currently begin widespread operations.[268] Even so, the wide spectrum of possible ADR methods reveals great promise, and many ADR projects are currently under way or are being planned for the near future.[269]

1. Contactless Active Debris Removal

Practical methods exist for actively removing pieces of space debris without the need for ever physically contacting the object. These methods seek to lower the orbital altitude of the debris by reducing its velocity,[270] thus exposing the debris to the cleansing effects of the lower LEO atmosphere. Such methods are desirable because they remove the risk of a collision between an ADR object and its space debris target.[271] However, they are slow to adjust their target's altitude[272] and are therefore generally best suited for small LEO debris.[273] Examples include focusing laser beams on the debris, or dispersing gas plumes, mists, or aerogels in space to artificially influence the atmosphere immediately surrounding the debris and therefore alter its velocity and altitude.[274] Additionally, ion-beam shepherds can be used to focus a plasma stream at a piece of debris to impart a propulsive force.[275]

The most promising contactless ADR method uses directed-energy beams, or lasers, to affect the orbital altitude of primarily smaller pieces of debris in LEO.[276] This can be accomplished in several ways and via ground or space-based lasers.[277] Low-intensity lasers can be used to affect the debris' velocity in the form of focused light pressure, much like the solar radiation already affecting space debris.[278] Higher intensity lasers, whether continuous or pulsating, can be focused on overhead debris to ablate the material, creating tiny, high-velocity ejections of plasma roughly perpendicular to the surface of the object, the thrust of which can be used to affect the debris' velocity and altitude.[279] However, significant technological hurdles remain. For example, calculating the exact orbital parameters of small debris fragments and then intersecting that debris with sustained and effective laser intensity requires highly precise tracking information and is, even then, complex and inexact.[280] Ultimately, incredibly difficult problems of laser intensity, pulse duration, tracking, and space situational awareness (SSA) must be overcome before widespread implementation is feasible.[281]

2. Capture and De-orbit/Re-orbit

While contactless ADR methods hold great promise, the primary approach currently under development is the physical capturing and de-orbiting or re-orbiting of the targeted space debris.[282] Once the ADR object makes physical contact with the space debris, the two objects become linked, for example via a tether or grappler, and the ADR object can then use its internal propulsion system to 'tug' the composite system to a new higher or lower orbit or even de-orbit it entirely.[283] Many different methods have been proposed to accomplish such a capture: nets, grappler tentacles, robotic arms, or even harpoons.[284] Some of these methods

have already undergone space-based, proof-of-concept testing. For example, RemoveDEBRIS, a U.K.-led and E.U. funded project, successfully harpooned a sample of a typical satellite panel affixed to an extended boom in 2019.[285]

In comparison to the contactless methods described previously, the physical capture of space debris comes with additional challenges. Since it necessarily requires the launching of an ADR object into space to make contact with the debris, there is significant expense involved.[286] This expense is compounded by the fact that most capture ADR methods are only designed to remove a single piece of debris.[287] In addition, physical capture ADR methods must overcome the difficult reality that it is common for space debris, especially large pieces, to be tumbling on an axis rather than orbiting smoothly.[288] Further, the debris object may have an unknown mass or center of mass or lack any fixture for easy grappling.[289] Physically linking up with tumbling or otherwise unstable debris with unknown orbital characteristics can be dangerous since it may result in unknown rotational forces after capture, ultimately increasing the risks of fragmentation and the creation of even more debris.[290] Ultimately, "rendezvous and interaction with an uncooperative and unprepared object has never been performed before."[291]

However, such methods also have some advantages. Unlike some contactless ADR methods, they are theoretically feasible for both large and small objects in all orbits, from LEO to GEO, assuming enough fuel is available.[292] Further, to alleviate the financial costs involved, some ADR capture and de-orbit devices have been proposed as a group of vehicles to clean up multiple pieces of space debris at the same time. For example, NASA has patented designs for capture-method ADR devices which can be augmented to contain up to eight individual de-orbiters within a single payload.[293]

3. Attachment of Active or Passive De-Orbit Aids

Distinct from physically capturing debris and re-orbiting or de-orbiting it through moving a composite system, others have proposed methods of ADR designed to approach into close proximity with or make physical contact with the target debris, but thereafter attach either an active or passive aid to hasten reentry. Most often, this attached de-orbit aid aims to interact with the limited atmosphere in LEO, thereby increasing its drag effect, or to make use of solar radiation or the Earth's geomagnetic field to affect the orbit of the targeted debris.[294] For example, some have proposed affixing long tethers to increase drag, whether by physical momentum exchange or through electro-dynamic forces.[295] Others have suggested using propelled nets to ensnare satellites and thereby increase atmospheric drag, as was done by the RemoveDEBRIS mission in 2018, utilizing a

mock satellite it released itself.[296] Still others have proposed solar or drag sails to slow and de-orbit debris.[297] In fact, the final on-orbit test for the RemoveDEBRIS project before reentry will be to employ such a drag sail to observe its effects on a reentering spacecraft.[298] Similar tests have already been successfully conducted in LEO, such as was done by the InflateSail project in 2017 with a much smaller CubeSat.[299] Other ideas include attaching inflatable balloons or even spraying the target debris with expanding aerogels, foams, sticky balls, or even freezing mists to increase surface area,[300] since the effect of atmospheric drag on debris is compounded if its area-to-mass ratio increases.[301]

These various methods still face challenges similar to the more standard 'capture' ADR methods. Specifically, they can still be quite complex and dangerous operations if the target piece of space debris is tumbling, has an unknown center mass, or lacks a stable fixture point.[302] Some fare better than others in this regard, since shooting foam or a drag net at debris from a stand-off distance is less risky than capturing and physically affixing a momentum exchange tether to it. Further, these methods are mostly appropriate and effective only for smaller debris in LEO.[303] Regardless, since the ADR object will not be using its on-board propulsion to move the composite system, this method faces another serious challenge in that the re-orbiting piece of debris will reenter the atmosphere in an uncontrolled fashion, possibly posing a danger to people or objects in flight or on the surface of the Earth.[304]

B. Legal Challenges Complicating Active Debris Removal

While many of the ADR technologies described above are theoretical, some are at or very near deployment-ready. However, the legal landscape in space is far from clear when it comes to ADR. In fact, several significant legal challenges complicate ADR and must be addressed by the international community prior to large scale ADR efforts being undertaken.

1. Definition of Space Debris

The first significant legal challenge inhibiting ADR is a threshold one: the lack of an international, legally binding definition of space debris.[305] As some have noted, "it may be easier to identify what is not space debris than to obtain agreement as to what it is."[306] In order to discuss the concept of space debris thus far, this article has employed the general IADC/COPUOS Guideline definition for simplicity, namely, all "man-made objects including fragments and elements thereof, in Earth orbit or re-entering the atmosphere, that are non-functional."[307] This definition was, notably, endorsed by the UNGA in 2007.[308] As such, it has

been described as the first broadly international definition for space debris.[309] However, this definition is limited to the context of the IADC and COPUOS Guidelines themselves, meaning that it has no binding legal applicability in relation to any international space law treaties or declarations.[310] This is problematic because none of the major U.N. space treaties or Declarations even mentions the term 'space debris' at all,[311] despite the clear OST requirements in Article IX to explore and use space, including the Moon and other celestial bodies, with "due regard" while avoiding its "harmful contamination."[312] Neither is there any coordinating body or regulatory agency to aid in their interpretation, as they were adopted across many years and by different sets of state parties.[313] The Liability and Registration Conventions speak only of "space objects," without ever distinguishing between functional and nonfunctional or useful and non-useful space objects.[314] They merely note that the term 'space object' "includes component parts of a space object as well as its launch vehicle and parts thereof.[315] Importantly, they are also silent when it comes to fragments of space objects.[316] Some consider this definition to be poorly crafted and vague, in that it is so broad as to extend to any "tangible human or even robotic-crafted matter or instrumentality in outer space."[317] If such an all-encompassing definition somehow excluded space debris, it would result in the perplexing conclusion that space debris is not governed by the current international space law regime at all, to include rules relating to international responsibility and liability for space objects.[318] Therefore, many argue that space debris should rightly be considered a subset of space objects under current international space law.[319]

The reason that a commonly agreed to and legally binding definition is so important is because it is not altogether clear what the term 'non-functional' necessarily means, or how being non-functional appreciably alters the legal characterization of a 'space object.' Specifically, core international space law concepts, like those concerning liability or jurisdiction and control, do not turn on a space object's functionality.[320] Since 'space objects' include component parts thereof, even if a space object is fragmented into pieces, those fragments are likely still space objects.[321] If these fundamental and well-settled principles of international space law are unaffected by a space object losing its functionality, it is hard to grasp what legal effect, if any, the COPUOS space debris definition intends to impart. In other words, if a non-functional payload remains a space object and therefore subject to the core legal principles of the international space law regime, what useful distinction is gained by declaring it to be 'space debris?'

Further, because of the lack of a *de jure* space debris definition, it is unclear what criteria should be applied when determining whether a given space object is functional or not. For example, is a non-maneuverable payload non-functional?

Maneuverability is seen by many to be a critical component of what is understood by the term 'functional,'[322] yet few would consider an otherwise functioning LEO CubeSat to constitute space debris simply because it lacked an on-board propulsion system. What if the space object retained its maneuverability but its sole probe was non-operational? Without an accepted, binding definition, these questions are difficult to answer. Even if the criteria were clear, it is not obvious who gets to make the functionality determination, which would likely, at least in part, turn on the space object's subjective value to its owner.[323] An otherwise non-functional satellite (whatever that means) may still be quite useful for discrete scientific purposes, for cannibalization, or even for space manufacturing.[324] For example, it could be scavenged for parts or utilized as a test satellite to hone on-orbit satellite servicing capabilities or ADR technologies. Therefore, being non-functional is not necessarily synonymous with being non-valuable, or, as some have put it, space debris does not necessarily mean "space waste."[325]

Additionally, if functionality is to define space debris, it is difficult for States to make this assessment properly, if at all, for objects not under their own jurisdiction and control. While States "shall … as soon as practicable" furnish basic information about their space objects to the U.N. under Article IV of the Registration Convention, many do not.[326] Others, like Russia, register payloads, but not discarded rocket bodies.[327] Further, while States "may" update the registration,[328] there is at present no legal requirement under international law to share the day-to-day functional status of satellites with other nations and certainly no state practice of such transparency.[329] In the national security context, it is understandable that States may be reluctant to volunteer up-to-date information about the functionality of their critical remote-sensing, communication, positioning, and early warning capabilities.[330] Therefore, without insider information, States may reasonably disagree on whether a given space object is truly non-functional, and therefore debris.[331]

Further, the IADC/COPUOS definition fails to include some arguably non-functional items in space that others tend to include. For example, non-manmade, or naturally occurring, objects in Earth orbit are exempted from the IADC/COPUOS definition of space debris. Despite this, some countries, for example the United States, prefer the term 'orbital debris,' which it defines to include non-manmade objects.[332] Additionally, objects not in orbit around the Earth or reentering the atmosphere are excluded from the category of space debris.[333] Therefore, a non-functional, manmade payload in orbit around the moon is, for whatever reason, not considered space debris under the IADC/COPUOS definition.

In short, the lack of an international, legally binding definition of space debris creates uncertainty about how to objectively identify space debris and how space debris is treated in relation to the laws surrounding space objects within the current international space law regime, specifically in terms of liability and jurisdiction and control. Instead, the only definition which has gained traction is not legally binding, is limited to the specific context of the IADC/COPOUOS Guidelines, and fails to clearly define its critical terms.

2. No Legal Duty to Prevent or Remove Space Debris

Another challenge inhibiting ADR is the failure of international space law to impose a clear legal obligation on States to avoid the creation of space debris or a duty to remove its own space debris. The first four U.N. space law treaties from the 1960s and 1970s laid the foundation of today's hard international space law, and little has changed since then.[334] Because none of these U.N. treaties discusses space debris *per se*, it has been questioned whether they directly apply to its creation or removal at all.[335] Many of the fundamental principles laid down in these treaties, especially the OST, are now considered customary international law.[336] Regardless, application of these specific principles to the problem of space debris is difficult, as they are likely too vague to support any international obligation to avoid the creation of space debris.[337] For example, it is not clear how the "due regard" principle or the "harmful contamination" principle from Article IX of the OST could or should be applied to the creation of space debris, since virtually all space missions release *some* debris. How much 'regard' should be given to other countries in relation to the creation of space debris? How much contamination via space debris is 'harmful interference?' The OST fails to provide clear answers both because it fails to define what these terms mean and because it is not at all clear that these specific provisions were ever intended to directly address the problem of space debris.[338]

It can be useful when struggling to apply international space law to the creation of space debris to consider not just the minimal or expected level of debris creation inherent in virtually all space missions, but to consider the most egregious or wanton acts of debris creation, such as ASAT tests.[339] If such a dramatic, intentional example does not violate international space law, it can hardly be said there is an affirmative duty to refrain from creating space debris. However, as already noted in Part II(D)(1), *supra,* the IADC/COPUOS Mitigation Guidelines afford States the discretion to conduct these intentional fragmentation events "when necessary."[340] While non-binding, these Guidelines are widely adopted and are therefore indicative of the *opinion juris* of nearly all space-faring States. Similarly, States have been reluctant to step forward themselves to condemn these

intentional debris-creating events as illegal under any substantive provision of customary international law or treaty law.[341] Therefore, even in the historically worst examples of intentional debris creation, ASAT tests, there is no clear consensus that a violation of an international obligation has taken place, severely undercutting any argument that public international space law forbids the creation of debris itself.

Some have suggested that the fundamental, underlying goals of the U.N. space treaties could arguably create some sort of an "implied" obligation to limit debris.[342] However, while perhaps in keeping with the collective spirit of the treaties, State practice belies this through repeated ASAT tests and the millions of pieces of space debris currently in Earth orbit. It is clear that the creation of space debris is not, in and of itself, illegal under international law.[343] Without a legal duty to refrain from creating space debris, there is, by extension, certainly no obligation to affirmatively remove space debris via ADR.[344]

Because no legal duty exists to refrain from creating space debris nor to remove one's space debris, there is little legal incentive for states to develop and field ADR technology. Indeed, a "tragedy of the commons" scenario arises wherein preventing or removing space debris is in the interest of all States, but few are willing to bear the costs because the legal regime does not require them to do so.[345] Therefore, despite the IADC and COPUOS Guidelines' recognition of the debris problem, without clear international legal obligations to avoid creating and to remove space debris, it is a challenge to motivate States to play their part in solving the debris problem.

3. Jurisdiction and Control of Space Debris

One of the most foundational concepts of early international space law is that the State of registry retains continuing "jurisdiction and control" over its space objects.[346] However, the application of this bedrock principle serves to frustrate the advancement of ADR.

a. Jurisdiction and Control under Current Space Law

The UNGA outlined the concept of "jurisdiction and control"—even before the adoption of the first U.N. space treaty—in its 1963 "Declaration of Legal Principles Governing the Activities of States in the Exploration and Use of Outer Space."[347] This document declared that the State "on whose registry an object launched into outer space is carried shall retain jurisdiction and control over such object, and any personnel thereon, while in outer space. Ownership of objects launched into

outer space, and of their component parts, is not affected by their passage through outer space or by their return to the Earth."[348] Several years later, in 1967, virtually identical language was reiterated in the OST.[349] However, the OST failed to clarify how such a registration was to be carried out. The Registration Convention remedied this in 1973 by explaining that the launching State of a space object launched into Earth orbit or beyond shall register it "by means of an entry in an appropriate registry which it shall maintain."[350] If there is more than one launching State, they "shall jointly determine" which single State will register the space object.[351] Determination of "the contents of each registry" and "the conditions under which it is maintained" was left to the individual States,[352] but certain information shall be passed onto the Secretary General for compilation in a U.N. Register.[353] Further, it defined the term "State of registry" as "a launching State on whose registry a space object is carried …."[354]

"Jurisdiction," in this context, entails the right of the State of registry to exert legal enforcement over and liability and responsibility for the space object, while "control" reserves to the State of registry the right to technically oversee and maneuver the space object.[355] Combined, the concept of "jurisdiction and control" provides States with a level of certainty over their space objects within an international legal regime that does not otherwise permit States to assert sovereignty in outer space, since Article II of the OST prohibits national appropriation through claims of sovereignty or any other means.[356] Critically, a State of registry's right to jurisdiction and control continues even if technical control over the space object is lost.[357]

b. Challenges for Active Debris Removal

The first and most obvious challenge posed to ADR by the legal concept of jurisdiction and control is that it establishes an exclusive hegemony over the space object for the registering State. In other words, no other State may interact with, rendezvous with, capture, or otherwise molest a space object without first obtaining the registering State's express permission.[358] Historically, this concept has proven itself quite useful, since any unilateral right to remove space objects, even seemingly abandoned or unimportant debris, would likely cause significant international conflict because of national security concerns, perhaps even leading to war.[359] However, obtaining the permission of a State to perform ADR on its space object would be a complicated endeavor, and may be denied or even ignored for any or no reason at all. Such permission is likely to become even more complicated if the relevant space object is owned by a private entity instead of the State itself. Further, there is currently no standardized mechanism or accepted international protocol for requesting and receiving permission for ADR activities.[360] The

natural result of this exclusivity is that, barring express permission, it limits the ADR efforts of countries to only those space objects under their own jurisdiction and control, or more specifically, those objects on its national registry. Limiting countries to ADR of only their own space objects restricts them from freely targeting the pieces of debris which will most help ameliorate the global debris problem, namely those with high collision probabilities which have the largest masses and surface areas and are located in the most congested orbits.[361] Without such freedom, global ADR efforts will be seriously stunted.

If express permission is denied, the legal concept of jurisdiction and control can also limit the number of potential nations conducting ADR. By number, approximately one-third of the space debris in orbit in 2011 was owned by the United States, one-third by Russia, and one-third by China.[362] Therefore, unless these three countries grant others permission to conduct ADR on their space objects, there are only a few major players who will even be legally permitted to tackle the debris problem through ADR, and none of them will be capable of doing it single-handedly.[363] With regard to mass, 70% of the total mass of space objects in LEO in 2014 belonged to Russia, primarily consisting of disused rocket bodies.[364] If Russia does not itself conduct ADR, which, as already discussed it has no obligation to do, and also refuses to give its permission for other countries to remove its space objects, the majority of the mass in LEO is legally untouchable because of the jurisdiction and control provision in Article VIII of the OST. Some have described this exclusivity as one of the most significant legal obstacles inhibiting ADR efforts.[365]

Not only is jurisdiction and control definitively established for the State of registry of a space object, the challenges for ADR are compounded by the fact that this exclusivity is ongoing. In other words, the right to jurisdiction and control does not end as long as the object is in space, so there is never temporal cessation of jurisdiction and control,[366] irrespective of the object's functionality.[367] This continuity raises questions regarding the transferability or abandonment of objects under a State's exclusive jurisdiction and control. Currently, there is no international space law mechanism for transferring jurisdiction and control of on-orbit space objects, so it is not surprising that there is scant State practice.[368] Even still, transfers have occurred before, albeit in limited numbers. For example, in 1997, the United Kingdom transferred ownership of three satellites to China concurrent with Hong Kong's return, thereafter notifying the U.N. that it had removed these satellites from its national registry.[369] China, conveniently also a launching State of these satellites, subsequently re-registered them on its own national registry and then informed the U.N.[370] However, the fact that there is no obligation for States which acquire on-orbit satellites to confirm the status

of their registration with the original launching States complicates matters, as does the lack of an obligation to report this change of ownership to the U.N. in order to amend the U.N. Register.[371] Without clear international obligations and consistent State practice in re-registering transfers, it may become difficult to determine which State possesses jurisdiction and control of a given space object, further complicating ADR. For this reason, the UNGA encouraged states to submit information on their practices regarding on-orbit transfer of ownership of space objects, with an eye towards harmonizing such practices.[372] Several years later, the Assembly expressly recommended that, upon any change in "supervision" of an on-orbit space object, the State of registry should notify the U.N. of the new operator and the date of the change.[373] It further recommended that, if there is no State of registry at the time of the change, the new operator should itself furnish that information.[374] Despite this, the possibility remains for difficulties and disputes regarding the registration, and thus, jurisdiction and control, of transferred space objects.[375]

Perhaps more important than transferability, the U.N. space treaties and declarations are silent about the possibility of legally renouncing or abandoning jurisdiction and control of one's space objects.[376] Further, there is no clearly recognized concept of abandonment of jurisdiction and control of a space object in practice in public international space law,[377] despite some notable authors arguing for the reasonableness of such an approach.[378] This is because Article VIII of the OST states that jurisdiction and control are continuous while in space and that ownership extends even after the object returns to the Earth. Therefore, legacy pieces of debris that are clearly unguided and non-functional, such as defunct payloads or rocket bodies left over from the 1960s, are still legally tied to their States of registry.[379] Without a recognized concept of abandonment of jurisdiction and control for uncontrolled debris that the State of registry has expressed a permanent intent not to recover or utilize, akin to derelict property in maritime law,[380] the fact that the State of registry retains exclusive sovereignty seriously inhibits the ADR efforts of other nations.

Further complicating ADR, the concept of jurisdiction and control arguably extends even to debris fragments,[381] meaning that States likely still possess sovereign control over the fragments of their formerly intact space objects. This is because pieces of space debris, as discussed in Part III(B)(1), *supra*, are still generally considered "space objects" under the U.N. space treaties. Further, while left undefined, Article VIII of the OST also expressly references its applicability to the "component parts" of space objects. However, despite the concept of jurisdiction and control likely applying to fragments, there is no express requirement to register fragments resulting from an on-orbit breakup.[382] Neither do States

accomplish this registration in practice. It would be surprising if, for example, China individually registered the thousands of trackable fragments from its 2007 ASAT test. In fact, registration practices are much less onerous; some States, such as Russia, interpret "space objects" to only mean payloads and therefore fail to even register their spent rocket bodies at all,[383] much less the many fragments of their exploded rocket bodies.

This general lack of registration of fragments, rocket bodies, and sometimes even functional payloads, leads to the final major problem regarding the concept of jurisdiction and control, namely that of attribution. Since in practice registration is far from consistent,[384] it can be difficult, if not impossible, to determine which State possesses jurisdiction and control of a given space object, especially in relation to debris fragments.[385] If jurisdiction and control applies to space objects in perpetuity, even arguably to fragments, and it is unclear which country has created or registered a specific piece of debris, then no State will *ever* be able to acquire the legal permission needed to remove it via ADR. It is worth noting that some have suggested the concept of jurisdiction and control should not apply to small pieces of debris, especially if it is no longer possible to determine its corresponding state of registry.[386] Regardless of these arguments, there is simply no State practice of removing unregistered space objects, further hindering ADR efforts.[387]

4. Liability for Space Debris

Another foundational concept of early international space law, liability for damage caused by space objects, is laid out in the Liability Convention of 1972. Unlike the concept of jurisdiction and control, liability for damage caused by a space object rests with the launching State or States.[388] Unfortunately, the application of such a liability regime in the ADR context creates legal uncertainty and discourages efforts to remove debris.[389]

a. Liability under Current Space Law

Just like jurisdiction and control, the UNGA outlined the concept of liability for space activities in its 1963 "Declaration of Legal Principles" by providing that each State which "launches or procures the launching of a space object" and each State "from whose territory or facility an object is launched" is "internationally liable for damage to a foreign State or its natural or juridical persons by such object or its component parts on the Earth, in air space, or in outer space."[390] This State or group of States are now known as the "launching State" or "launching States."[391] Several years later, in 1967, virtually identical language was reiterated in the OST.[392] However, both the UNGA and the OST failed to elaborate on the

application of international liability for space activities with any specificity. The Liability Convention remedied this in 1972 by clarifying via *lex specialis* that a launching State is "absolutely liable" for any damage caused by its space object or component parts on the "surface of the Earth or to an aircraft in flight," but only liable for damage caused elsewhere, *i.e.* in space, if the damage is due to "its fault or the fault of persons for whom it is responsible."[393] The Convention limits its damage to injuries to people and property,[394] thereby excluding generalized damage to the outer space environment itself.[395] Thus, a dual liability regime is created, either absolute or fault-based, depending on where the damage occurs. However, no definition or standards for fault are provided, nor is any standard of care prescribed.[396] The Liability Convention also maintains the four-pronged OST definition of a launching State, namely the State which launches or procures the launch, or the State from whose facility or territory the launch occurs.[397]

It is important to note that modern space objects often have more than a single launching State and can sometimes have as many as four or more,[398] the identities of which may or may not be entirely transparent to the international community.[399] Three launching States would result under the Liability Convention, for example, in the case of a French company procuring the launch of its satellite through a Russian spaceport located in Kazakhstan. In cases of damage caused by a space object with more than one launching State, all are jointly and severally liable.[400] Relevant for the ADR context, if space object A, launched by State A, is damaged through a collision with space object B, launched by State B, thereafter causing damage to a third party, whether on Earth or in space, then State A and State B are jointly and severally liable according to the general liability rules from Article II and III, with the burden of compensation apportioned based on comparative fault.[401] If the relative degree of fault is unknown or cannot be apportioned between States A and B, then liability will be apportioned equally.[402]

Finally, it is also important to note that the term "space objects" as defined by Article I(d) of the Liability Convention arguably includes the fragments of space objects resulting from on-orbit breakups.[403] This is because any other interpretation would create a significant, virtually fatal, lacuna in the international space liability regime, since no State would then be responsible for damage caused by the debris fragments which total nearly 53% of all space objects.[404] Therefore, damage resulting from, for example, any of the thousands of small fragments resulting from a space collision or an ASAT test, may also subject the original launching State or States to liability.

b. Unique Risks of Active Debris Removal Related to Liability

Before discussing the challenges posed by this liability regime as it relates to ADR, it is important to consider that ADR is an inherently risky undertaking, since all ADR technologies require some form of interaction with space debris.[405] More often than not, this interaction takes the form of a direct physical connection between objects co-located in space. In LEO, that means linking up objects which may be traveling with velocities in excess of 30,000 kilometers per hour, or over 8 kilometers per second.[406] Such on-orbit rendezvous or docking maneuvers are already complex for stable, controlled objects, much less for pieces of space debris which may be unguided, tumbling, lacking any obvious grapple point or docking mechanism, physically degraded, or even full of volatile residual fuel.[407] Further, the resultant movement of the joint, post-capture system can be quite unpredictable, especially as the center of mass of the debris is not necessarily known.[408] All of these challenges with direct-capture ADR methods increase the risk of an accidental on-orbit fragmentation event,[409] possibly resulting in the creation of more debris or even runaway liability.

Even in circumstances without physical capture, such as through the use of directed-energy lasers, ADR is not without additional risks. A longer-than necessary laser pulse (just near a millisecond) risks over-ablating the debris material, creating "splashing" and potentially even more debris.[410] Further, since the laser must necessarily cross through other space orbits, it has the potential to accidentally illuminate functional spacecraft, which can damage or degrade sensitive on-board optical sensors.[411] Also, laser-based ADR methods will, by design, result in the uncontrolled reentry of space debris. If any part of the debris survives reentry, it inherently poses a threat to aircraft in flight and to people and property on the surface of the Earth.

Finally, ADR, by its nature and purpose, alters the orbital altitude of targeted space debris. In doing so, the space debris will inevitably pass through the orbits of other space objects either on its own or in tandem with its controlling ADR object, thereby increasing the risk for conjunction events.[412] Some have suggested that this creates the need for an ADR traffic management system which can apprise other space operators of the up-to-date orbital characteristics for the ADR object's transitory path, especially for ADR objects which will conduct repeated or continual maneuvers, such as the proposed ElectroDynamic Debris Eliminator, or EDDE.[413]

c. Challenges for Active Debris Removal

Because ADR increases the risk for further fragmentation and damage to other objects in space and people and objects on the surface of the Earth, as discussed above, the current space liability regime creates several specific challenges for the development of ADR.

In order to explore these challenges, consider the following, completely plausible, ADR scenario. Assume that a single State, State A, launches and later registers a defunct rocket stage in upper LEO orbiting at 1,200 kilometers in altitude. A second State, State B, requests and receives express permission from State A to conduct ADR on the rocket body. Thereafter, State B launches an ADR object, captures the rocket body, deorbits it to 400 kilometers, and then releases it to naturally decay and reenter the Earth's atmosphere. State B's ADR object then deorbits itself and burns up entirely upon reentry. Two weeks after the ADR mission concludes, the rocket body, still orbiting at roughly 400 kilometers, explodes for an unknown reason and a large piece of the resultant debris strikes the ISS, destroying the station and killing five astronauts from three different countries. Given the regime established under the Liability Convention, it is unclear which State would bear international liability for this damage. Since the damage occurred in outer space, the launching State of the space object causing the damage is liable if the damage is due to its fault or the fault of persons for whom it is responsible.[414] But whose fault is the damage? State A left an arguably dangerous piece of space debris behind in orbit where it could harm other space objects and astronauts, as it ultimately did. However, State B, with the permission of State A, captured this debris and moved it down to a lower, but crowded, orbit which enabled it to harm the ISS. What about the explosion? Without more information, which may be impossible to acquire, there is no way to know whether the explosion would have occurred if the debris was left alone or if State B's capture and de-orbiting was somehow deficient, itself causing the explosion to occur. It is impossible to determine on these facts whether State A or State B, or perhaps both, is at fault for this damage, especially without an explanation for the explosion and some legally enunciated standard of care. Yet other States and their astronauts have obviously suffered damage and should be entitled to compensation. Further, how are we to factor into the current liability rules that State B was, separate and apart from the fragmentation event and ultimate damage, doing the world a great service by attempting to shorten the orbital lifetime of the debris?

This hypothetical highlights the striking ambiguity that results when the current international space law liability rules are applied to an ADR scenario. This legal ambiguity creates several significant disincentives in relation to ADR, both for the launching State(s) of the targeted debris object and the launching State(s) of the ADR object.

First, the current liability rules disincentivize States from conducting ADR on their own space objects. As argued above, ADR itself increases the chance of additional fragmentation and damage. Therefore, launching States face a lower likelihood of eventual liability if they simply ignore their space debris and leave it on-orbit. Even if the space debris breaks up on-orbit and its fragments cause damage to another State's space object, it is unlikely to result in liability. This is because the onus is on the claimant State to prove causation, and thus attribution of the fragment and the identification of its launching State(s), in addition to fault or negligence,[415] burdens which, due to the remoteness of outer space, may be practically impossible to carry.[416] Even if these burdens were able to be carried, in practice the Liability Convention has never been invoked in relation to damage caused by debris fragments in space, only on the face of the Earth.[417] Therefore, the liability regime disincentivizes States from conducting ADR on their own debris.

Second, the liability rules, and specifically their ambiguity, create a disincentive on the part of the State of registry of the debris (which will be, in virtually all cases, also a launching State[418]) to authorize other States to conduct ADR on their debris. Specifically, if an accident were to occur during direct capture ADR, thereby causing damage to the space object of a third party, it is not immediately clear whether, under Article IV of the Liability Convention, the launching State(s) of the ADR object or the launching State(s) of the targeted space debris would be most at fault. This is, in part, because it is not clear what fault looks like under the Liability Convention. Does simply launching a satellite which later becomes debris itself amount to negligence under the Liability Convention's fault-based regime for space damage?[419] On the one hand, since all space missions release at least *some* amount of debris, it seems unreasonable that the leaving behind of debris is, in and of itself, negligent in relation to any damage it may cause at a later time during an ADR accident.[420] On the other hand, while it has been near universal state practice, leaving a multi-ton, pressurized, unguided rocket body to float around a congested orbit for 50 years does not seem like something a prudent actor should do, especially if the technology exists to avoid doing so in certain orbits. This ambiguity under the liability rules is created because the Liability Convention fails to set out any standard of care or method for determining fault.[421] Further, since the Liability Convention has only been invoked once in the nearly 50 years since its inception, and even then only for damage to the Earth,[422] there is no indication

from any sitting tribunal of what standard of negligence is appropriate to apply in relation to damage in space from ADR activities. In circumstances of uncontrolled reentry of space debris, for example from contactless ADR methods like ground-based lasers, the question of who bears the fault may not even be relevant. Instead, since there is technically only one space object involved, the launching State(s) of the debris would be absolutely liable under the Liability Convention if the reentering debris caused damage on the surface of the Earth.[423] Therefore, in such cases, the launching State(s) of the piece of debris, not the State controlling the ADR laser, will bear 100% of the risk of liability resulting from the ADR mission. For these two reasons, even if a well-meaning State offered to conduct ADR on the space debris of another State, the debris-creating State may not be inclined to accept an increased risk of damage under circumstances of unclear or one-sided liability.

Third, not only does the current liability regime deter ADR from the perspective of the launching State(s) of the debris in multiple ways, it also disincentivizes other well-meaning States from ever even offering to conduct ADR on their behalf. This is because the ADR object is, generally speaking, the active participant in the interaction with and re-orbiting/de-orbiting of an otherwise uncontrolled, but trackable and largely predictable, debris object. Therefore, even though it may be argued that leaving behind debris is itself negligent, it is just as reasonable to argue that the launching State(s) of the ADR object has considerably more control and influence over what occurs during the ADR attempt. In that sense, the launching State(s) of the ADR object could reasonably be found to be more at fault for any mishap during the ADR process which causes damage and apportioned the majority of the liability, especially if damage results after the orbit of the space debris has already been adjusted by the ADR object, as in the hypothetical described above. If the launching State(s) of ADR objects arguably stand to bear a larger share of the liability for any damages occurring while conducting ADR on the space debris of other States, there is an obvious legal disincentive to undertake such activities.

These three significant disincentives are further exacerbated by the fact that there is no recognized international mechanism for launching States to transfer their liability for a space object to another State.[424] In the ADR context, this means that States are unable to transfer liability for their own space debris even to a willing ADR State. As has been observed, "once a launching State is always a launching State."[425] In practice this means that if a State's territory is used to launch a space object, even if that State played no part in procuring or conducting the launch whatsoever and no part in operating or controlling the space object thereafter, it is jointly and severally responsible along with any other launching States for any damage caused by that space object in perpetuity under the terms of the Liability Convention. This illogical apportionment of liability is a commonly

criticized aspect of the current space law regime.[426] It appears that the drafters of the Liability Convention did not foresee private space operators or on-orbit satellite sales[427] and premised their liability rules on the erroneous assumption that the launching State would be singular and would always have undisputed physical control of the relevant space object.[428] In order to cope with this regime, States and private space operators must circumvent the Liability Convention by utilizing complex systems of private, bilateral indemnification agreements, as expressly permitted in Article V.[429] These agreements are only binding between the individual parties, so the States remain liable under the Liability Convention in public international space law.[430] Despite these agreements, the structural defect in the Liability Convention and its impediment to ADR efforts remains.

Overall, the ambiguity surrounding liability for ADR missions and the resulting disincentives are significant legal challenges which complicate and inhibit ADR efforts. Not surprisingly, Dr. Joseph Pelton, a prolific space academic and industry professional, has called the rules surrounding the Liability Convention the "largest legal barrier to efficient orbital debris removal."[431] Unless and until these are adjusted or clarified, ADR efforts are likely to be stifled into the future.

5. Export Control Laws

Another significant legal obstruction inhibiting ADR is the proliferation of nationally and internationally imposed export control laws, primarily in the way such laws operate to inhibit the transfer of space technology and stifle international cooperation to accomplish ADR. In short, export controls are designed to restrict the shipment or transmission, styled an "export," of controlled military or dual-use materials, goods, services, or technologies outside of the country or to foreign operators in any location.[432] Importantly, they can also apply to the "re-export" of such items, even by foreign actors, such as is the case in the United States if such items contain U.S.-origin components or technology.[433] These export restrictions are often premised on strategic interests, especially during wartime, as well as concerns for foreign policy, nuclear non-proliferation, or combating terrorism.[434] Export controls commonly apply to various types of space-related technology, especially satellite and satellite components and launch systems. In combination with the continuing jurisdiction and control of registered space debris, as discussed in Part III(B)(3), *supra*, these export controls make it much more difficult for States to grant permission to other countries to perform ADR on their space debris, especially if it contains any U.S.-origin component or technology.[435] This is because granting a foreign entity the right to access, capture, and control a piece of space debris (and therefore any on-board items or technology) for ADR purposes, even if only momentary, would fall within the scope of an "export" within most

export control laws because, in order to be effective, this term is often defined in strikingly broad terms.[436] Even the simple sharing of technical data to enable such a mission could violate export control laws.[437] Therefore, even if State A is willing to absorb the liability risks and financial costs required to deorbit State B's space debris, State B may have adopted national laws or agreed to international arrangements which ban it from granting permission for or aiding such a mission, either outright or without first obtaining special authorizations. Most modern space-faring nations, including Canada,[438] France,[439] India,[440] Russia,[441] China,[442] and many others maintain some form of export controls.[443] Without question, the most restrictive country in the world in terms of export controls, whether in general or specifically as it relates to space technology, is the United States through its sprawling International Traffic in Arms Regulations (ITAR) and Export Administration Regulations (EAR).[444] These overlapping, comprehensive export control rules are so pervasive that they have led to a demand in the global space market for the development of "ITAR-free," and therefore freely tradeable, satellites,[445] and have even had the unintended effect of stimulating the Chinese rocket and satellite industries.[446]

Restrictive export control laws are not just limited to domestic legislation; they have even cropped up through international arrangements to limit the transfer of and access to sensitive weapons and dual-use technologies. For example, while less restrictive than the U.S. system, the European Union maintains a collective set of export controls which specifically includes various types of space technology.[447] Additionally, more than 40 countries have banded together under the so-called Wassenaar Arrangement, a non-binding, multinational agreement which creates a comprehensive export control regime for many dual-use items.[448] The current list of Wassenaar-controlled dual-use goods, technologies, and munitions restricts the transfer of numerous types of space launch vehicles and spacecraft, including their components.[449]

In conclusion, these various export control restrictions, whether imposed by national law or adopted internationally, serve to inhibit ADR efforts when combined with the jurisdiction and control rules from Article VIII of the OST. The aggressive export rules of one country, for example the U.S., may even inhibit other countries from agreeing amongst themselves to remove space debris, due to the extraterritorial application of reexport rules within these export control laws. Of course, these are not absolutely fatal to ADR; exceptions to export control laws may generally be made at the agency or national level, on a case-by-case basis. Regardless, they all work together to create a complex web of global restrictions which constrain states from freely, or at least inexpensively and expeditiously, granting their permission for other states to conduct ADR on their space debris.

6. Regulatory Vacuum

Space debris and the necessary ADR response are significant global public policy matters that should be of universal concern. So far, the most visible efforts to tackle the problem have been conducted through the IADC and COPUOS, but only as it relates to mitigating new space debris. As already noted, this has proved insufficient. A regulatory agency with the mandate to address this problem through ADR has not yet emerged in the international sphere. Despite the creation of international space law treaties and the evolution of customary international space law, as yet there is no clear international agency in charge of space safety, space traffic management (STM), or other space debris-related concerns.[450] While there are international agencies which deal with regulating certain aspects of space, such as the ITU with respect to frequency allocation, harmful radio interference and GEO slot management,[451] no single agency coordinates the ADR operations discussed in this article. This regulatory void has caused the United States, a major global space-power to call for deeper global engagement through bilateral and multilateral discussions and through existing international organizations, specifically in relation to STM and standards on behavior surrounding the space debris environment.[452]

Without some sort of centralized, global organization to coordinate international ADR efforts, or possibly even to conduct ADR itself,[453] it is difficult to imagine that States will be able to overcome the fundamental legal challenges to ADR already discussed, such as jurisdiction and control issues, liability issues, or export control restrictions. Further, even if these issues were worked out, there is no agency to ensure space safety and traffic management for ADR efforts, which will almost certainly include navigating through various orbital planes.

Until some form of international regulatory framework is developed, ideally through a new comprehensive, multilateral space agreement, it is "unlikely that substantial progress can be made with regard to a coordinated approach to ADR."[454]

C. Policy Challenges to Active Debris Removal

In addition to the lacunae and rigid foundational concepts embedded in the U.N. space treaties, as well as overlapping national and international export control regimes, there are two major policy issues which also inhibit the development of ADR. Specifically, these include economic and strategic challenges.

1. Economic Challenges

Like many other uniquely global challenges, the question of economics plays a central role in the efficacy of ADR operations. As noted in Part III(B)(4)(b), *supra*, since most ADR concepts anticipate launching an ADR payload into space to make physical contact with the target debris, an ADR mission will generally be an expensive endeavor. It will contain all of the research and development costs, licensing costs, insurance costs, launch costs, ground-station costs, and operational costs that any traditional space venture would include.[455] However, the end result will obviously not include any commercial space application to sell or license, such as television broadcasting or Earth observation, to recover these costs. Further, while it may develop in the future, there is currently no global market for providing hireable ADR services. Additionally, since most proposed ADR concepts anticipate only deorbiting a single piece of debris across the life of the ADR object, many ADR operations would be unable to spread the costs across deorbiting several pieces of debris, making each mission incredibly expensive.[456] Given the lack of convertible income stream, at least at the current time, and the limited utility of individual, "single-debris" missions, some have argued that all current ADR systems now available "suffer from a 'business case' that lacks a clear and solid economic rationale for their use.[457] Regardless of such blanket statements, it is incredibly difficult to cost a "typical" ADR mission, since they can vary infinitely in the number of targets, size of targets, distance of orbital adjustment, and method of ADR,[458] yet ADR must still compete against other, obviously cheaper alternatives.

For example, the conceptual costs of intervening only at the last minute to alter debris orbits through micro, gas-induced orbital adjustments, so-called "just-in-time collision avoidance," would likely amount to only U.S. $1-3 million per launch, meaning it could theoretically be as much as 1,000 times cheaper than the cost of an average ADR operation.[459] This determination is made by calculating the average cost of reducing one on-orbit collision. Since ADR operations are premised on the concept of reducing collisions through the wholesale cleanup of space, it could take the removal of approximately 35-50 pieces of space debris to reduce a single collision, totaling anywhere from U.S. $300 million to U.S. $3 billion per collision reduction.[460] Separate and apart from the costs of ADR missions, studies have also been conducted to determine the relative value to be gained by removing a piece of debris and thereby reducing the chances of needing to replace an operational payload due to a destructive collision event. In one such study from 2013, it was estimated that removing a small satellite in sun-synchronous orbit would only return a "value" worth approximately U.S. $14,500 on average, compared with U.S. $306,000 for the removal of a large, 2,000 kilogram piece of debris.[461] If the

relative costs for ADR operations remain too high and the monetary benefit derived from removing debris objects remains too low, it may result in the unfortunate conclusion that it is simply easier to just keep launching replacement satellites than to remove defunct ones,[462] making it hard for States to justify the economic costs of fielding ADR systems.

Given the global nature of the space debris problem, it is also unclear which States should pay for the high costs of ADR. Should all nations contribute equally for ADR operations since the space debris problem is a global one? Perhaps that is appropriate, but probably not, in light of the fact that the overwhelming majority of the space debris currently in Earth orbit was created by relatively few nations, most prolifically the USSR/Russia, China, and the United States.[463] It is arguably unfair to require States which have never created a single piece of debris to subsidize the historical environmental negligence of other, more industrialized, ones. This argument has repeatedly been made in the international climate change arena and has come to be known as "common but differentiated responsibilities."[464] Such a concept appears highly relevant to ADR and the space debris problem. Even if it were clear which States should be putting up the money to conduct ADR, other policy questions inevitably emerge. For example, should the cost of ADR be borne upfront at the time of launch or provided later, when it comes time to actually remove the piece of debris? Additionally, with commercial enterprises comprising a larger and larger percentage of modern space activity, how much of the costs for ADR could or should be shifted to the commercial space industry as opposed to being borne by States themselves? Should the space participant who created a particular piece of space debris be responsible for removing it, whether civilian or government? Individual responsibility seems to be the fairest solution but becomes problematic if the participant, whether civilian or government, is unable or unwilling to pay for the debris to be removed. Overall, these economic policy challenges related to ADR do not have readily apparent solutions. Much more will need to be discussed and agreed to by global players, likely by and through regulatory organizations, global ADR funds, launch taxes, or through new or modified international instruments before the financial aspects of ADR can be settled.

2. Strategic Challenges

Another critical policy challenge facing ADR is the fact that most ADR technologies are also capable of being used nefariously.[465] In other words, any method of physically capturing, affixing objects to, or repositioning a piece of space debris could similarly be used to capture an enemy satellite, affix a weapon or intelligence device to it, alter its orbit, or simply disrupt or destroy it.[466] Because of this, virtually all ADR methods are considered "dual-use" technology,[467] since they could

also be utilized as ASAT "space weapons."[468] Their development and use can be seen by some countries as the creation or refinement of on-orbit ASAT technology and, therefore, a threat to their freedom of use of space for important strategic, primarily national defense, purposes.[469] So, as ADR technology is perfected and proliferated to solve the debris problem, it simultaneously and problematically increases global strategic fears of its misuse, threatening to further militarize, or even weaponize, the space domain.

Very similar to the jurisdiction and control and liability issues discussed in Parts II(B)(3) and (4), *supra,* these strategic challenges make it less likely that States would be willing to permit a foreign state, especially a perceived adversary, to remove pieces of its space debris.[470] Even worse, it may make States skeptical of ADR technology altogether. To ameliorate these strategic fears, States will likely need to engage in information exchanges and transparency and confidence-building measures, perhaps through an ADR-focused international regulatory organization.

D. Conclusion

Other than the fact that ADR is absolutely necessary to stabilize the space environment, much remains unclear about ADR technology and its eventual implementation in outer space. The current proposals for various methods of ADR are incredibly varied, from lasers to harpoons to nets to solar sails. While some are closer to implementation, virtually all require further development and testing.

As the technology matures, serious legal and policy challenges must be addressed before ADR can be implemented on any meaningful scale. Most of the legal challenges stem from the legacy U.N. space law treaties which make up the specialized field of international public space law. As a threshold matter, since there is no mention of space debris at all in this regime, it appears that debris concerns were not being seriously considered at the time of drafting. Without a definition of and clear legal obligations in relation to debris, it is difficult to adequately deal with the space debris problem at the international level. Legal challenges also flow directly from the foundational legal concepts of these treaties, such as "jurisdiction and control" and the core liability principles. It remains to be seen how ADR will be conducted without relaxing the jurisdiction and control rules or further clarifying the principles of liability, especially as they may apply to fault-based damage in outer space during ADR operations. Further, the application of these concepts to non-State, commercial actors must be clarified. Notwithstanding these legal challenges, ADR operations otherwise face considerable policy challenges regarding financial feasibility and strategic distrust over "dual-use" technologies.

IV. Future Strategies

Given the importance of ADR operations to the stability of outer space and the significant legal and policy challenges inhibiting them, it is critical that the global community rapidly develops strategies to facilitate ADR. No longer can the world community afford complacency in the face of the rapid growth of space debris, hoping that lukewarm compliance with mitigation guidelines will magically reverse the more than 60-year trend. It must make prompt and decisive changes to the international space law regime, developing a *lex ferenda* which both clarifies and encourages ADR. However, the nature of the debris problem is such that no one State or small group of States can adequately solve it alone. Therefore, while States should not be complacent in their domestic space initiatives, comprehensive and radical international solutions must be prioritized. It is the contention of this article that the swiftest and most comprehensive way to accomplish this goal is through the drafting and widespread adoption of a new multinational space treaty. Using the challenges to ADR discussed in Part III as a guide, Part IV will address how such a new treaty should be structured to facilitate ADR in the future.

A. New Space Treaty

The most direct method of overcoming the legal challenges related to ADR would be to draft an entirely new international space treaty focusing specifically on the issue of debris. The most obvious place to negotiate a new space treaty would be through COPUOS, where each of the previous space treaties has originated. Unfortunately, this process can be painfully slow and generally operates only via consensus.[471] Some have worried that the consensus needed to adopt a new treaty through COPUOS would render it too diluted to be effective.[472] Partly because of this, Christopher Williams has suggested the possibility of bypassing COPUOS as a forum altogether and instead negotiating a binding multinational instrument amongst only the active space-faring nations, thereby generating an instrument which might later be used as a template for a future COPUOS agreement.[473] Williams believes that such a course of action could have the benefit of speeding up negotiations since they could be limited to "only knowledgeable States," more easily avoiding "being sidetracked by tangential issues."[474] Regardless of how the treaty itself may come about, such a new, comprehensive space compact should be constructed incorporating the principles presented below.

1. *Mandate* Compliance with COPUOS Guidelines

As argued in Part II, stabilizing the LEO space environment requires not only the implementation of effective ADR, but also continued, strict adherence to the

COPUOS Mitigation Guidelines, especially regarding post-mission disposal.[475] Because of this, any new treaty addressing the space debris problem should extend beyond hortatory language simply reemphasizing the importance of member States adopting the guidelines, as COPUOS and the UNGA have repeatedly done throughout the years.[476] Instead, it must include language whereby States agree to be internationally bound by the COPUOS Guidelines. The elevation of the Guidelines to a treaty obligation will transcend the inevitable precatory nature of a guideline regime and have a more likely prospect of generating higher levels of compliance by States in the future.

2. *Define* Space Debris

Any new space treaty must develop a clear definition of space debris, specifically as it relates to controllability, communication, and functionality.[477] The relationship of these attributes to space objects can dramatically expand or contract the scope of what is internationally considered to be debris. For example, a control-based definition alone would arguably be overbroad, since it would include all unguided space objects, whether functional or not. While the current, non-binding IADC/COPUOS definition hinges on functionality and may therefore be more appropriate,[478] it still remains unworkable. The concept of "functionality" is, by itself, inadequate to legally delineate what is and is not space debris, especially in a world where the capability to service or refuel a nonfunctional satellite through OOS is rapidly maturing. Therefore, space debris must be further defined. If it is not, problems will arise in situations where States or commercial entities still have practical uses planned for currently non-functioning satellites.

Arguably, any new treaty definition of space debris should clarify that all fragments resulting from collisions, explosions, or unknown breakup events, which together total more than 53% of all tracked space objects,[479] should be categorically considered space debris. Post-fragmentation, they are certainly of quite limited use and are most likely entirely non-functional. The remaining bulk of the tracked space objects, notably intact but non-functional payloads and expended rocket bodies, arguably have some future potential use or "functionality," whether it be via the extension of usable life through OOS or simply salvage operations. Acknowledging this abstract, future functionality makes it difficult to declare such material to be space debris in such a way that any other State may capture and de-orbit/re-orbit it without authorization. Therefore, when defining space debris in a new multinational treaty, it will be necessary to define a time-period after the loss of functionality within which a State must somehow utilize the space object or forfeit exclusive jurisdiction and control over it. While admittedly an arbitrary time span, this article suggests adopting the IADC/COUPUS Guidelines' 25-year

timeline for post-mission de-orbiting of LEO payloads. In that regard, any intact but non-functional object not utilized by its State of registry within 25 years of becoming non-functional should be considered space debris, regardless of any potential future uses for the object. However, it must be acknowledged that, even under this clarified definition of space debris, transparency surrounding the point at which a space object loses its functionality remains problematic due to the difficulty of obtaining accurate data for often secretive outer space systems.

More than simply defining what space debris is, however, a new treaty must also adequately situate the notion of debris in the context of the prior U.N. space law treaties. Imperatively, this means clarifying in binding fashion whether or not space debris, however defined, is a subset of space objects,[480] especially when it comes to the fragments resulting from on-orbit explosions, ASAT tests, or conjunction events. This is crucial because, if space debris is a subset of space objects, then the State of registry retains jurisdiction and control of that debris under the OST and the Registration Convention, even if the resultant debris is shattered into thousands of fragments. However, if space debris is not a subset of space objects, then the problematic jurisdiction and control and liability concepts found in previous U.N. space treaties would simply not apply to it.[481] In other words, once a space object becomes space debris, the right of the State of registry to exert jurisdiction and control over it ceases, such that any State may conduct ADR on it. The latter interpretation is much preferred, as it can provide the significant legal flexibility required to disregard the unhelpful traditional rules of liability and jurisdiction and control applicable to space objects and develop more appropriate long-term rules for space debris to facilitate ADR. At the same time, the decades-old system that States have come to rely upon for traditional space objects would be retained, preserving the necessary order amongst States with functioning satellites.[482] For this reason, any new space treaty negotiated to address space debris should declare that it does not fall within the confines of Article VIII of the OST, meaning that the State of registry no longer retains jurisdiction and control over a space object once it becomes debris. Similarly, any new treaty should clarify that space debris falls outside the definition of a space object for purposes of Article I(d) of the Liability Convention and thereafter enunciate the liability regime applicable to space debris independent of traditional space objects and in a manner which encourages ADR.

3. *Clarify* International Obligations Regarding Space Debris

A new space treaty should also clearly express binding obligations on States in relation to space debris creation or space debris removal. Currently, as discussed in Part III(B)(2), no such obligations exist. Ideally, a new space treaty would contain a binding obligation to refrain from the creation of debris

altogether and an obligation to clean up any created debris. Unfortunately, an outright ban on any debris creation or an obligation to clean up all created debris is currently unrealistic, as it is too ambitious for the state of current technology, including both space launch technology and ADR technology. Neither would such a ban/obligation dyad comport with the prevailing political environment. However, a new space treaty should at least seek to extend the principles found in the IADC/COPUOS Guidelines in order to ban, rather than merely discourage, the *intentional* destruction of space objects, at least during peacetime and outside of situations involving self-defense to an imminent threat or use of force, thus making illegal the kinetic destruction of satellites via direct ascent ASATs. This is critical because these intentional breakups can create vast amounts of extremely long-lasting space debris fragments. As noted previously, the 2007 Chinese ASAT test currently accounts for the single largest fragmentation event in space history.[483] Similar to the way that nuclear testing has been banned via international treaty in certain locations,[484] outer space is a unique environment that should be shielded from military testing which is seriously deleterious to its future operational use, as kinetic ASAT tests arguably are.

Even if States cannot agree on sweeping obligations banning space debris or kinetic ASAT tests, new treaty negotiations should consider other, less onerous, ways to facilitate ADR through binding obligations related to debris. For example, a new treaty should include an affirmative obligation to update the U.N. registry entry when a payload becomes nonfunctional debris. Doing so would force international transparency for ADR operations, since States would be responsible for publicly "declaring" their national space debris. It would also transparently begin the proposed 25-year period within which the State must utilize the space object's latent functionality or lose exclusive jurisdiction and control over it. Additionally, it would be helpful for attributional purposes to set a timeline for registering newly launched space objects with the U.N., or even a requirement to register the observable fragments of one's national debris. Finally, States could consent to be bound under international law to remove a small portion, perhaps as low as 1% or even a single intact piece, of their own space debris each year,[485] similar to binding carbon emission reduction targets. This would go a long way towards stabilizing the LEO environment, as NASA's data shows that removing merely five pieces of debris could significantly alter the total debris population in the future by reducing the frequency of conjunction events.[486]

4. *Adjust* Liability Rules for Space Debris

If space debris is no longer considered a space object, the liability regime established by the Liability Convention no longer applies to space debris. As such,

new liability rules must be established under the replacement regime. First and foremost, to properly incentivize ADR, any new space treaty must be clear that liability for damage caused by space debris is no longer permanently tethered to the "launching State" as defined in Article I(c) of the Liability Convention. As argued in Part III (B)(4), this outdated rule makes little sense in today's highly cosmopolitan, commercially-dominated space industry. Instead, liability should be clarified to flow to the State of registry at the time the space object becomes debris. If there is no State of registry at that time, liability should rest with the State which last maintained operational control over the object. In this way, the State liable for damage caused by the space debris is appropriately the State that registered it or actually controlled it, rather than a "launching State" which may have merely provided the territory or facility for its original launch.

Further, the standard of liability for damage caused by single debris objects and single ADR objects in space should be clarified and should incentivize ADR operations. For example, the liability standard applied to debris-creating States should be adjusted. Specifically, the standard of liability applied to the debris-creating State for damage caused in outer space by its debris should be heightened from fault-based to a rebuttable presumption of fault or even to absolute liability, as it already is for damage caused on the surface of the Earth. This would increase the potential liability of States for damage caused by its debris in space and therefore disincentivize the creation of new debris. In the opposite vein, the liability standard applied to States for damage caused by ADR objects should similarly be adjusted in a new space treaty. Specifically, rather than the current nebulous "fault" standard for liability, damage caused by a single ADR object should be held to a lessened standard, such as requiring an injured party to show wanton or gross negligence on the part of the ADR operator, or even have liability for potential damages suspended entirely.[487] This reduced liability standard for ADR objects is premised both on the general need to incentivize ADR operations, but also a recognition of the service that ADR ultimately provides to all space-faring nations.

Apart from adjusting the liability standards for damages caused by single pieces of space debris or single ADR objects, it would also be wise for any new space treaty to address the composite systems which are uniquely and inevitably created by predominant capture ADR methods. If an ADR object and a piece of captured space debris are operating as a conjoined system and jointly cause damage to a third party or in the process of conjoining collide into one another and thereafter cause damage to a third party, the traditional Liability Convention rules would consider the responsible states jointly and severally liable, but apportion the burden of compensation based on comparative fault.[488] However, as demonstrated by the hypothetical ADR damage scenario in Part III, a fundamental flaw in the current

liability regime is that it is incredibly difficult, and often impossible, to determine precisely which party is at fault for damages flowing from delicate ADR operations conducted in outer space. Therefore, any new treaty addressing space debris should simply avoid the confusion and impossible burden of proof involved in determining comparative fault for these situations. Instead, when it comes to damages arguably caused by both the ADR and its targeted space debris, it should automatically apportion liability equally between the State of registry or the operating States for both the ADR object and the piece of space debris, rather than expecting States to demonstrate their share of the comparative fault. This clarity flowing from streamlining the liability rules will remove much of the unknown liability exposure for ADR operations inherent in the current regime.

Finally, to bring the liability regime in line with the modern era of private, commercial space ventures, any new space treaty should include provisions affording States the ability to formally transfer liability for their space debris to any other State which is willing to conduct ADR or else specifically authorize cross-waivers of liability for ADR operations,[489] similar to the private arrangements authorized under Article V of the Liability Convention.

Ideally, States should agree to apply these liability rules retroactively to previously launched space objects. Not only would this be more effective in that it would cover the entirety of the currently existing space debris, but it would also obviate the need to distinguish between debris created prior to and after the adoption of any new liability standard. However, even if States only agreed to apply them prospectively, each of these adjustments to the liability regime surrounding space debris would still operate to disincentivize the creation of space debris, while at the same time incentivizing its active removal.

5. *Authorize* the Abandonment of Space Objects

Any new space treaty should also include language to clearly permit States which no longer wish to limit ADR from third parties to effectively abandon their space objects in some way.[490] Permitting a state to, as the renowned space law Professor Bin Cheng called it, "disown"[491] jurisdiction and control over its space objects would greatly increase the ability of other States willing to conduct ADR on those objects to do so. It would also erase the 25-year waiting period discussed above in circumstances where a State has no intention of ever utilizing a nonfunctional space object in the future. Ideally, in order to maximally facilitate ADR, the treaty should also establish a public, international registry, similar to that established by the Registration Convention, to consolidate information related to all such abandoned or disowned debris objects.[492]

6. *Establish* a Global ADR Organization

Any new space treaty addressing debris should also commission a global regulatory agency or organization to coordinate and regulate global ADR efforts. Options for the structure and mission of such a global ADR entity are endless: it could be an organization to exchange legal and technological information, conduct ADR research, establish best practices or guidelines for ADR (in much the same way the IADC has with space debris mitigation), manage and distribute ADR funds, assist with SSA or STM, coordinate global ADR efforts, settle ADR disputes, help select ADR candidate targets, or even to actually conduct ADR operations itself.

Professor Ram Jakhu and space professionals Yaw Otu Nyampong and Tommaso Sgobba have jointly suggested an intergovernmental organization structure that also directly incorporates public and private space operators, akin to the models used for the International Telecommunications Satellite Organization (INTELSAT) or the International Maritime Satellite Organization (INMARSAT) in the 1960s and 1970s.[493] Such a blended structure could prove to be uniquely advantageous for ADR efforts, because any organization solely comprised of States or their space agencies would fail to include a significant and growing portion of the space industry, namely private operators. No ADR strategy or solution to the debris problem can be successful without integrating and coordinating with the private space industry.

However, other commentators have suggested alternative structures. For example, Agatha Akers has proposed a U.N.-designated research "center" to spearhead ADR efforts.[494] Alternatively, already existing organizations can be a potential avenue to fill this regulatory void for ADR. There has been recent discussion about expanding several currently-existing organizations to regulate many parts of future space activities, such as STM, safety, or environmental pollution, and from a variety of established international agencies, such as the International Civil Aviation Organization (ICAO), the ITU, or the World Meteorological Organization (WMO).[495] ICAO, a specialized agency of the U.N. which oversees the safety and security of international civil aviation, has received more attention than others, especially in the realm of STM,[496] largely due to the emergence of suborbital flights reigniting the age-old debate of the boundary between air space and outer space.[497] However, ICAO could theoretically be tasked to regulate space traffic as high as GEO.[498] If an organization like ICAO is assigned more space related functions in the future, such as in relation to suborbital STM, perhaps it can be empowered in a new U.N. space treaty to also take on the task of acting as a global forum for ADR operations and related safety issues.[499] Beyond the remit of the aforementioned organizations, the IADC, an intergovernmental organization

made up of all of the major space-faring nations and dedicated to the issue of space debris, is another natural international forum within which to discuss ADR coordination and regulation efforts.

Regardless of the structure of the forum, any organization established by a new space treaty should be specifically empowered to raise funds for ADR (discussed *infra*), select ADR targets, and conduct ADR operations on space debris. The outsourcing of target selection and removal to an international, treaty-based ADR organization is critical to minimizing the strategic concerns of States over the potential weaponization of ADR technology.[500] If the multinational organization is in charge of selecting ADR targets and/or controlling the ADR operations, nations will have less cause for concern that a rogue State would abuse or exploit ADR operations. Further, if empowered to select targets, the organization would be in a position to focus ADR operations on the least strategic and least controversial pieces of debris, or even on completely unattributable debris, thereby building international confidence and transparency for centralized ADR operations.[501]

7. *Empower* the ADR Organization to Raise Funds

As noted in Part III(C)(1), *supra*, ADR operations are not currently economically viable and are subject to a "tragedy of the commons" problem. Therefore, authorizing a newly created ADR organization to raise money in order to diffuse the subsidization of removal efforts is paramount.

Perhaps the simplest way of collecting revenues for a global ADR fund would be to include provisions in the new space treaty which authorize the established ADR organization to promulgate a process for the imposition of a global tax to be levied against either States or commercial entities for the launching of space objects,[502] sometimes styled a "space access fee."[503] This type of fee would have the benefit of shifting the majority of the costs associated with ADR to those States and commercial entities which launch the most space objects. However, given all of the variables and unknowns when it comes to the creation of space debris and ADR operations, it is incredibly difficult to determine an appropriate or optimal tax amount per launch.[504] Agatha Akers has suggested a simple flat-rate fee of U.S. $5 million for each unmanned object launched into space and U.S. $1 million for each manned space launch.[505] Others, such as Molly Macauley or Joseph Pelton, have considered basing the tax off a percentage of the production or operational costs of the spacecraft and launch vehicle, suggesting figures anywhere from a fraction of a percent[506] to roughly 5%,[507] this range being multiple times lower than what is commonly paid in launch insurance costs.[508] Zhuang Tian has pointed out that the mass of the launched object and its eventual orbital altitude

should be factored into the tax, since larger objects are more likely to fragment into many more pieces and will remain in orbit longer at higher altitudes.[509] It could also be useful to scale the tax based on the relative probability or risk of collision for specific intended orbits. In other words, the more congested or hazardous the orbit, the higher the tax should likely be.[510] Finally, it could also be beneficial to provide discounts on the front end or rebates on the back end for deorbiting, graveyarding, shielding, installing maneuvering capability, or any other desirous debris mitigation strategies.[511] Such a scheme would work to increase compliance with mitigation guidelines while simultaneously generating revenues to further global ADR efforts.

While a launch tax would be the simplest and preferred method to raise global funds for ADR efforts, a new space treaty could alternatively be negotiated to directly establish economic contributions to the ADR organization from various countries.[512] These contributions could be effectuated in multiple ways. Joseph Imburgia and Timothy Nelson have suggested basing a State's monetary contribution on its relative proportion of the space debris population, akin to a market-share or "polluter pays" principle.[513] However, this would quickly limit the pool of contributors to only space-faring nations, and would also require enormous, upfront contributions from just three or four countries which may be unwilling or unable to satisfy their share of the costs.[514] Alternatively, it has been suggested that all countries which are space-faring nations as well as all those which partake in the benefits of space use and exploration should contribute to the global fund.[515] These contributions could instead be apportioned equitably,[516] similar to the approach adopted by major climate change treaties in regards to carbon emissions,[517] whereby the more industrialized nations contribute the most capital.

Clearly, there are a myriad of ways in which to structure a fee or tax on space access or utilization. Regardless of the method ultimately employed, any new space treaty must seriously address the economics of space debris by empowering the global organization to generate funds to subsidize ADR.

B. An Alternative Approach: Space Treaty Protocols

Any realistic discussion of a new space treaty must confront the fact that no widely adopted space treaty has been created in almost 45 years. Therefore, a comprehensive treaty addressing space debris faces stiff challenges.[518] There is arguably too little political will or desire to presently conclude such a multinational agreement.[519]

However, even if a completely new space treaty regarding space debris is unpalatable, many of the same or similar adjustments discussed above can be made to the existing treaty regime through limited protocols to the current U.N. treaties. Again, a precondition for such changes would be a viable, binding legal definition of space debris. However, after the definition and legal status of debris is clear, the liability or jurisdiction and control rules applicable to such debris could be modified in piecemeal fashion, separate and apart from those rules that apply to "space objects," so long as enough States would be willing to agree to the changes. While a comprehensive space debris treaty is optimal, even modest adjustments to these treaties could seriously aid future ADR efforts, for example by simply updating the Registration Convention to set a deadline for registering a space object or by a binding obligation to provide updates after orbital movements or fragmentation events,[520] thereby clarifying the status of space objects and their controlling State. While even a protocol to a U.N. space treaty may seem farfetched, some U.S. politicians have publicly stated that it may be time to revise some of the concepts contained in the OST, especially in relation to the widespread growth of commercial space operators.[521]

C. Concurrent National Efforts

During the negotiation and conclusion of a new space treaty or protocol, States should not sit idly by; they must themselves take aggressive domestic steps to further ADR efforts. These will most easily take the form of requirements embedded in the national licensing systems that most States have enacted pursuant to Article VI of the OST, which requires States to authorize and continually supervise the space activities of their non-governmental entities, but could also take the form of taxes or punitive measures.

1. Licensing Requirements for Active Debris Removal

States can quickly and easily amend their national licensing requirements to overcome some of the challenges inhibiting ADR operations, in much the same way that many have done for space debris mitigation efforts.[522] In essence, States may enact licensing laws and regulations which prescribe preconditions on space activities or require their national space operators to take certain measures or to conduct their space activities in certain ways.

As the simplest example, in order to overcome the lack of an international obligation to remove one's own space debris, a State may simply make debris removal a license condition. In other words, the domestic license required to launch an object into outer space can be conditioned on the license holder agreeing

to remove any resulting space debris related to that object, a so-called "assured removal clause"[523] or "assured removal requirement."[524] However, such a licensing provision could only feasibly be applied to a payload and perhaps its rocket stages, since the mandated removal of microparticulate exhaust particles or paint flecks or thousands of fragments from an on-orbit explosion or collision is not economically realistic nor even currently possible. Alternatively, a State could require a potential licensee to either prove an adequate level of solvency or to carry an insurance policy in an appropriate amount to cover the costs of paying the State or a third-party company to conduct ADR to remove any resulting debris.[525] Similar insurance conditions on licenses are already commonplace when it comes to off-setting potential liability for causing damage to persons or property.[526] Finally, States could even reserve for themselves the right to order the license holder to conduct or pay for ADR in an appropriate situation, to be determined by the licensing state on a case by case basis.[527]

States should also make legislative changes within other domestic licensing regimes. For example, they could choose to make exceptions in the domestic legislation or regulations which govern their export controls to authorize the "export" of certain space-related products and technologies without a license for the express and limited purpose of destruction of the debris via ADR-assisted deorbiting. This would obviate the need to apply for and receive an approved license for the export, which as noted in Part III(B)(5), *supra*, can be confusing, costly, and time consuming.[528] Even carving out just a partial exception, such as for only the least sensitive information and technology, would support ADR operations, especially from the United States since most satellites have at least some U.S. export-controlled technology or subcomponents.[529]

The primary benefit of embedding these kinds of conditions into national licensing laws is that the State can thus mandate ADR for objects under its own jurisdiction and control. In this regard, so long as the operation is conducted by an ADR object from the same nation, huge inhibitors of ADR can be avoided, namely the pernicious liability and jurisdiction and control mechanisms of the U.N. space treaties and export control laws.

While amending national space policy, lawmakers should take notice that many national licensing regimes do not apply to governmental space activities, especially military ones, and some even exempt certain government sponsored civilian space activities.[530] Because of this, merely amending a State's domestic space licensing provisions would fail to capture the entirety of its national space operations. In order to fill that gap, States should establish separate guidelines for those excepted government entities to require similar ADR operations, since most space agencies

and intergovernmental organizations still comply with various other governmental measures or guidelines regulating their activities.[531] As an example, while the U.S. Department of Defense does not require a license to launch its space objects, it still must adhere to the U.S. Government Orbital Debris Mitigation Standard Practices.[532] Thus, while perhaps not subject to the traditional national licensing process, government activities can still be required to promote ADR operations.

2. Taxes/Sanctions

Similar to the idea of funding a global ADR operations via launch taxes, individual States should impose their own launch fee or launch tax in order to fund their national ADR efforts. In essence, every space launch by a national of that State or occurring from its territory or facilities could be required to pay a mandated surcharge, which can then be applied toward debris removal efforts. The collected resources could be utilized to support a national pledge of reducing a certain percentage of the State's existing space debris per annum. Alternatively, it could fund ADR research or subsidize or offset the costs of national or private ADR efforts. As previously described, various rebates to this national tax could also be returned for the proper disposal of a space object at its end of life or for compliance with other desirable mitigation measures, like shielding or graveyarding.

Alternatively, instead of a flat tax or tax and rebate structure, punitive sanctions could be imposed for the intentional or negligent creation of space debris. For example, the failure to properly deorbit a payload at its end of life could be met with a fine, perhaps scalable to the size of the resulting debris or the relative dangerousness of its orbit. Finances raised from these punitive sanctions could be used to further supplement the national ADR operations described above.

One benefit of establishing taxes and sanctions at the national level is that these measures can be instituted relatively quickly and with minimal international coordination while treaty or protocol negotiations are still ongoing. At the same time, these measures could form a starting point for groups of States to coordinate and regionalize similar actions, with an eye towards the possibility of eventually forming a global launch fee for ADR, as discussed above.[533] For example, it is not inconceivable that a domestic launch tax unilaterally imposed by an ESA member State might inspire other ESA States to follow suit and eventually to be adopted by all ESA States, perhaps even setting a precedent for inclusion in the new space treaty or protocol.

One potential drawback of such a national launch tax or sanction structure is that early adopting States may inadvertently discourage space launches by their citizens or from their territory and facilities, since they will have created additional costs and punitive regulations that might otherwise be avoidable by simply relocating the space activities. Therefore, until a truly global solution is instituted through a multilateral space treaty, it would be important to determine precisely what level of launch fees or debris sanctions would create a sustainable additional cost for a nation's space industry, while at the same time generating sufficient revenues to adequately subsidize national ADR efforts.

D. Conclusion

To comprehensively address the debris problem in a way that clarifies and incentivizes future ADR efforts, it is critical that States modernize the international space law regime surrounding debris through a new multilateral space debris treaty. Such a treaty must address the major challenges facing ADR efforts: it must compel compliance with COPUOS Mitigation Guidelines; adequately define space debris; clarify debris obligations; alter and alleviate the dual strangleholds of liability and jurisdiction and control; authorize the abandonment of space objects; establish an international regulatory agency for ADR; and create a funding mechanism for the agency's global ADR efforts. If global consensus cannot be reached on such a sweeping treaty, these individual issues must be tackled in piecemeal fashion through protocols to the existing U.N. space treaties. During what is likely to be a lengthy negotiation process for these changes, individual space-faring States still have a role to play. Until global solutions are realized, they should update their domestic space licensing and taxation laws in ways which incentivize and raise resources for national ADR operations.

V. Conclusion

The congestion of usable Earth orbits with space debris has been many decades in the making. While some are more responsible than others, all space-faring nations have contributed to this debris problem, only a modest portion of which is even observable to mankind. The rampancy of debris has only worsened over time, whether measured by mass or number of pieces of debris. Since widespread recognition of the problem in the early 1990s, the world has witnessed verified on-orbit collisions between space debris and functional satellites, collisions between actual payloads, and numerous intentional, sometimes catastrophic, kinetic ASAT tests. It has also observed a rapid increase in the number of space-faring nations and the maturation of a commercial space industry, both further exacerbating and complicating the space debris problem.

In the face of this unchecked debris growth, significant advances have been made towards practices aimed at mitigating the creation of new debris. Decades of work through multinational space organizations and the U.N. have ultimately resulted in widely adopted mitigation guidelines, as well as the standardization of spacecraft designs, operation, and disposal. However, these laudable efforts suffer greatly from serious conceptual failures internal to the guidelines, as well as from poor compliance rates. Ultimately, they have proven insufficient. Even assuming perfect compliance with these mitigation measures and the unrealistic hope of zero additional explosions or collisions in space, the debris population will continue to grow, especially in critical areas of LEO. Active debris removal, or the process of capturing debris and relocating it to either a disposal orbit or effectuating its reentry, is therefore necessary to stabilize the space environment and must be carried out as soon as possible.

However, the international space law regime failed to anticipate the problem of space debris and the rise of non-governmental space actors. It is therefore ill-suited to administer the operationalization of widespread ADR efforts. Long-standing, fundamental space law principles embedded in the seminal U.N. space law treaties stand in the way of effective global ADR. International space law needs to clearly define and situate space debris within its legal structure, or else risk paralysis by would-be ADR actors for fear of undertaking unknown or excessive liability or of violating the rights of other States. It must address and update, if necessary, the concept of "launching States" and their never-ending liability for damage, as well as modernize the currently unworkable liability regime. It must develop mechanisms which loosen the grip of jurisdiction and control of space objects by their States of registry. It must adopt and integrate new legal concepts which enable and facilitate the abandonment or transfer of space objects. Further, it must grapple with the lack of a coordinating agency for global ADR efforts and the nationally and internationally imposed export controls which pervade the space industry and stifle ADR. Overlapping these significant legal constraints are the enormous costs which must be shouldered to clean up the space environment and the distrustful national security apparatuses which must be convinced that ADR objects are not secret weapons.

Going forward, states, national space agencies, intergovernmental agencies, and multinational space organizations should begin considering adjustments to this stifling international space law regime, ideally through a new multinational space debris treaty or ADR-positive protocols to existing treaties. At the very least, they must begin to develop a regulatory regime which facilities ADR, hopefully via an ADR-coordinating global agency, whether created from scratch through international agreements or assigned to a currently existing entity, such as ICAO.

This agency needs to be empowered to raise funds to stimulate ADR technology, subsidize ADR efforts, and perhaps even conduct ADR itself. At the same time, individual States should be taking local measures to adjust their own licensing requirements to facilitate and encourage ADR, while at the same time instituting new launch taxes or even sanctions for the creation of debris. These legal and policy challenges are no small tasks, but they must be tackled in order facilitate ADR and preserve the long-term sustainability of our precious Earth orbits.

Endnotes

[1] *Space Environment Statistics*, Eur. Space Agency, Payload Launch Traffic into 200 hp 1750km, https://sdup.esoc.esa.int/discosweb/statistics/ (last visited Oct. 2, 2020).

[2] T.S. Kelso, *SATCAT Boxscore*, CelesTrak, https://www.celestrak.com/satcat/boxscore.php (last visited Oct. 5, 2020).

[3] J.-C. Liou & H. Cowardin, *NASA Orbital Debris Program Office and the DebrisSat Project* 5, Nat'l Aeronautics & Space Admin. [hereinafter NASA] (2018), https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20180001502.pdf, *cf.* Cody Chiles, *18 SPCS Now Predicts Debris-on-Debris Collisions in Space, Enhancing Space Domain Awareness for All*, Combined Force Space Component Command (CFSCC) (Sept. 24, 2020), https://www.spacecom.mil/News/Article-Display/Article/2360595/18-spcs-now-predicts-debris-on-debris-collisions-in-space-enhancing-space-domain/.

[4] *Space Debris by the Numbers*, Eur. Space Agency, https://www.esa.int/Safety_Security/Space_Debris/Space_debris_by_the_numbers (last updated Feb. 2020).

[5] *See, e.g.*, Donald J. Kessler & Burton G. Cour-Palais, *Collision Frequency of Artificial Satellites: The Creation of a Debris Belt*, 83:A6 J. Geophysical Res. 2637 (1978). NASA founded its Orbital Debris Program Office one year after this article was published, in 1979.

[6] For a brief overview of these efforts, *see* NASA, *Orbital Debris Management & Risk Mitigation* 24 (undated), https://www.nasa.gov/pdf/692076main_Orbital_Debris_Management_and_Risk_Mitigation.pdf. For a thorough description of the creation of the IADC, *see* Nicholas Johnson, *Origin of the Inter-Agency Space Debris Coordination Committee*, *in* ARES Biennial Report 2011-2012, 70-72 (2014), https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20140011750.pdf.

[7] *Monthly Object Type Charts by Number and Mass*, 22:1 Orbital Debris Q. News 10-11 (Feb. 2018), https://orbitaldebris.jsc.nasa.gov/quarterly-news/pdfs/odqnv22i1.pdf.

[8] For ESA's justification for designating active debris removal as a "strategic goal," *see Active Debris Removal*, Eur. Space Agency, http://www.esa.int/Safety_Security/Space_Debris/Active_debris_removal (last visited Oct. 2, 2020).

[9] More specifically, ADR is used throughout this article to describe the process of "rendezvousing, capturing, stabilizing, towing, transferring to a disposal/graveyard orbit or relocating, and de-orbiting through orbital maneuvers for active or passive re-entry into the Earth's atmosphere." *See* Ram S. Jakhu et al., *Regulatory Framework and Organization for Space Debris Removal and On-Orbit Servicing of Satellites*, 4:3-4 J. Space Safety Eng'g 129, 130 (2017).

[10] Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, Jan. 27, 1967, 18 U.S.T. 2410, 610 U.N.T.S. 205 [hereinafter Outer Space Treaty or OST].

[11] Convention on International Liability for Damage Caused by Space Objects, Mar. 29, 1972, 24 U.S.T. 2389, 961 U.N.T.S. 187 [hereinafter Liability Convention].

[12] Agreement on the Rescue of Astronauts, the Return of Astronauts and Return of Objects Launched into Outer Space, Dec. 19, 1967, 19 U.S.T. 7570, 672 U.N.T.S. 119 [hereinafter Rescue and Return Agreement].

[13] Convention on Registration of Objects Launched into Outer Space, Nov. 12, 1974, 28 U.S.T. 695, 1023 U.N.T.S. 15 [hereinafter Registration Convention].

[14] Agreement Governing the Activities of States on the Moon and other Celestial Bodies, Dec. 5, 1979, 1363 U.N.T.S. 3 [hereinafter Moon Agreement]. Note that, while the other four U.N. Space Treaties have garnered wide-spread acceptance, the Moon Agreement has secured only 18 ratifications as of 1 January 2020. For a comprehensive list of adherents to each of the UN Space Treaties, as well as several other international space-related agreements, *see* U.N. Office of Outer Space Affairs, *Status of International Agreements Relating to Activities in Outer Space as at 1 January 2020*, https://www.unoosa.org/documents/pdf/spacelaw/treatystatus/TreatiesStatus-2020E.pdf.

[15] For a comprehensive review of these soft-law mechanisms in international space law, *see* Francis Lyall & Paul B. Larsen, Space Law: A Treatise 33-48 (2d ed. 2018).

[16] *See, e.g.,* System, Apparatus, and Method for Active Debris Removal, U.S. Patent No. 9,555,905 (issued Jan. 31, 2017).

[17] *See, e.g.*, Tereza Pultarova, *Watch a Satellite Fire a Harpoon in Space in Wild Debris-Catching Test (Video)*, Space (Feb. 18, 2019), https://www.space.com/space-junk-harpoon-removedebris-satellite-video.html; Jonathan Amos, *RemoveDebris: UK Satellite Nets 'Space Junk'*, BBC (Sept. 19, 2018), https://www.bbc.com/news/science-environment-45565815.

[18] OOS refers to the "capability of refueling, repairing, or upgrading satellites that have become non-functional while in space." By extending the functional life of the satellite, OOS is technically "a means of … space debris remediation." *See* Jakhu et al., *supra* note 9, at 130.

[19] As such, this article does not specifically address the threats posed by naturally existing micrometeoroid debris nor any methods to address those threats.

[20] Rep. of the Comm. on the Peaceful Uses of Outer Space at Annex 1, ¶ 1, U.N. Doc. A/62/20 (2007), adopted by the UNGA in G.A. Res. 62/217, International Cooperation in the Peaceful Uses of Outer Space (Feb. 1, 2008); IADC, IADC-02-01, Rev. 1, *IADC Space Debris Mitigation Guidelines* ¶ 3.1, (Sept. 2007). For a critical analysis of some of the legal challenges associated with this definition in relation to ADR, see Comm. on the Peaceful Uses of Outer Space, Science and Technical Subcomm., *Active Debris Removal – An Essential Mechanism for Ensuring the Safety and Sustainability of Outer Space*, at 30-32, U.N. Doc. A/AC.105/C.1/2012/CRP.16 (2012).

[21] NASA Orbital Debris Program Office, NASA/TM-2018-220037, History of On-Orbit Satellite Fragmentations 3 (15th ed., 2018), https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20180008451.pdf; Nicholas L. Johnson, *The Earth Satellite Population: Official Growth and Constituents, in* Preservation of Near-Earth Space for Future Generations 18 (John A. Simpson ed., 1994).

[22] History of On-Orbit Satellite Fragmentations, *supra* note 21, at 3, fig.1.0-2; *Active Debris Removal, supra* note 20, at 16-17.

[23] *Orbital Debris Management*, *supra* note 6, at 6; Johnson, *supra* note 21, at 18.

[24] *Orbital Debris Management*, *supra* note 6, at 3; *Annual Space Environment Report*, GEN-DB-LOG-00288-OPS-SD, Eur. Space Agency 50 (Sept. 29, 2020), https://www.sdo.esoc.esa.int/environment_report/Space_Environment_Report_latest.pdf.

[25] *Orbital Debris Management*, *supra* note 6, at 3.

[26] *Id.*; *Active Debris Removal, supra* note 20, at 16-17.

[27] Johnson, *supra* note 21, at 18.

[28] *Orbital Debris Management*, *supra* note 6, at 6.

[29] History of On-Orbit Satellite Fragmentations, *supra* note 21, at 8.

[30] *Historical Growth of Space Debris* 3, Union of Concerned Scientists (2009), https://www.ucsusa.org/sites/default/files/2019-10/Debris-growth-graph-5-18-09.ppt.

[31] History of On-Orbit Satellite Fragmentations, *supra* note 21, at 3.

[32] *Id.*; Johnson, *supra* note 21, at 17-18.

[33] History of On-Orbit Satellite Fragmentations, *supra* note 21, at 12; Johnson, *supra* note 21, at 17-18.

[34] History of On-Orbit Satellite Fragmentations, *supra* note 21, at 12.

[35] *Id.* at *i*. This includes a combination of 242 breakup events and 78 anomalous events. *But see Annual Space Environment Report*, *supra* note 24, at 53 for ESA's differing sum of 561 such on-orbit satellite fragmentation events.

[36] *About Space Debris*, Eur. Space Agency, https://www.esa.int/Safety_Security/Space_Debris/About_space_debris (last visited Oct. 2, 2020).

[37] *Id.*

[38] *Orbital Debris Management*, *supra* note 6, at 12.

[39] *Position Paper on Space Debris Mitigation: Implementing Zero Debris Creation Zones,* SP-1301, 15, Eur. Space Agency (Feb. 2006), http://www.esa.int/esapub/sp/sp1301/sp1301.pdf. This is not an insignificant source of microparticulate debris, as the ESA estimated in the same document that that there were over 63,000m2 of painted surfaces orbiting the Earth in 2006.

[40] *Id.* at 7.

[41] *Orbital Debris Management*, *supra* note 6, at 11.

[42] Liou & Cowardin, *supra* note 3, at 5.

[43] J.-C. Liou, *Risk from Orbital Debris* 6*,* NASA (Nov. 9, 2018), https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20180008560.pdf.

[44] History of On-Orbit Satellite Fragmentations, *supra* note 21, at 3.

[45] *About Space Debris*, *supra* note 36. *But see id.* at 1 for NASA's claim that this figure actually stands at more than 75%, which would translate to more than 4,000 non-functional orbiting payloads.

[46] *Space Debris by the Numbers*, *supra* note 4.

[47] *Active Debris Removal, supra* note 20, at 17.

[48] *Orbital Debris Management*, *supra* note 6, at 6.

[49] Brian Weeden, *Tackling Space Debris Head On*, 26:7 Phys. World 17, 18 (2013).

[50] Rada Popova & Volker Schaus, *The Legal Framework for Space Debris Remediation as a Tool for Sustainability in Outer Space*, 5:2 Aerospace 55 at 2 (2018).

[51] Comm. On the Peaceful Uses of Outer Space, Sci. & Tech. Subcomm., *Towards Long-Term Sustainability of Space Activities: Overcoming the Challenges of Space Debris*, U.N. Doc. A/AC.105/C.1/2011/CRP.14, at 12 (2011).

[52] J.-C. Liou, *USA Space Debris Environment, Operations, and Research* Updates 9, NASA (2018), https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20180001749.pdf. It is important to note that highly sensitive individual sensors are capable of observing much smaller space objects. However, without multiple such sensors being positioned around the world to gather accurate orbital tracking data, these objects are only temporarily observed rather than continuously tracked by the SSN. *See Towards Long-Term Sustainability, supra* note 51, at 13. For a graphical representation of this advanced capability in the U.S., *see* Liou & Cowardin, *supra* note 3, at 10.

[53] Stew Magnuson, *News From Space Symposium: Tracking Objects in Space Both Easier, More Complicated*, Nat'l Def. Mag., Apr. 11, 2019, http://www.nationaldefensemagazine.org/articles/2019/4/11/tracking-objects-in-space-both-easier-more-complicated; *Space Fence Declared IOC and OA*, U.S. Space Force (Mar. 27, 2020), https://www.spaceforce.mil/Multimedia/Photos/igphoto/2002271462/.

[54] Popova & Schaus, *supra* note 50, at 2.

[55] Lesley Jane Smith, *Legal Aspects of Satellite Navigation*, *in* Handbook of Space Law 556-566 (Frans von der Dunk & Fabio Tronchetti eds., 2015).

[56] Brian Weeden et al., *Global Space Situational Awareness Sensors* 9, ResearchGate (2015), https://www.researchgate.net/publication/228787139_Global_Space_Situational_Awareness_Sensors; U.S., *Fact Sheet: Ground-Based Electro-Optical Deep Space Surveillance*, Air Force Space Command (Mar. 22, 2017), https://www.afspc.af.mil/About-Us/Fact-Sheets/Article/249016/ground-based-electro-optical-deep-space-surveillance/.

[57] *Towards Long-Term Sustainability*, *supra* note 51, at 12.

[58] Johnson, *supra* note 21, at 18.

[59] *Space Debris Mitigation Guidelines*, *supra* note 20, ¶ 5.3.1.

[60] Weeden et al., *supra* note 56, at 9; *Towards Long-Term Sustainability*, *supra* note 51, at 12.

[61] *Towards Long-Term Sustainability*, *supra* note 51, at 13. ESA's Optical Ground Station (OGS) in Tenerife, Spain operates a telescope which can reportedly detect, but not track, objects as small as 30 centimeters near GEO, but it is not operated exclusively for this function. *See* T. Schildknecht et al., *Optical Observations of Space Debris in High-Altitude Orbits,* Proc. 4th Eur. Conf. on Space Debris, SP-587, 113, 118, Eur. Space Agency (2005), https://conference.sdo.esoc.esa.int/proceedings/sdc4/paper/113/SDC4-paper113.pdf.

[62] Chiles, *supra* note 3.

[63] Johnson, *supra* note 21, at 10.

[64] Kelso, *supra* note 2; For a graphical representation of all SSN-catalogued objects, both currently on-orbit and previously decayed, *see* T.S. Kelso, *SATCAT Growth*, CelesTrak (accessed Apr. 30, 2019), https://www.celestrak.com/satcat/growth.png.

[65] *UCS Satellite Database*, Union of Concerned Scientists, https://www.ucsusa.org/nuclear-weapons/space-weapons/satellite-database#.WhyVnVNrw2x (last updated Apr. 1, 2020).

[66] *Id.*

[67] For a description of these models, as well as the statistical models used by JAXA, ISRO, ASI, and UKSA, *see Stability of the Future LEO Environment*, IADC-12-08, Rev. 1, IADC (Jan. 2013), at 5-7.

[68] *Towards Long-Term Sustainability*, *supra* note 51, at 14; Popova & Schaus, *supra* note 50, at 2.

[69] *Space Debris by the Numbers*, *supra* note 4.

[70] *Id.*

[71] *Towards Long-Term Sustainability*, *supra* note 51, at 17.

[72] *Space Environment Statistics*, *supra* note 1, Count Evolution by Object Orbit.

[73] *Space Environmental Statistics, supra* note 1, Mass Evolution by Object Orbit.

[74] *Monthly Object Type Charts by Number and Mass*, *supra* note 7, at 10-11.

[75] *Id.*

[76] *Space Environment Statistics*, *supra* note 1, Mass Evolution by Object Orbit; *Orbital Debris Management*, *supra* note 6, at 6.

[77] *Active Debris Removal*, *supra* note 20, at 15.

[78] *Id.*

[79] *See generally* F. Alby et al., *Collision of CERISE with Space Debris*, Proc. 2d Eur. Conf. on Space Debris, SP-393, 589-96, Eur. Space Agency (1996), https://conference.sdo.esoc.esa.int/proceedings/sdc2/paper/30/SDC2-paper30.pdf.

[80] History of On-Orbit Satellite Fragmentations, *supra* note 21, at 400.

[81] Nicholas Johnson, *First Natural Collision of Cataloged Earth Satellites*, 1:2 Orbital Debris Q. News 1-2, Sept. 1996, https://orbitaldebris.jsc.nasa.gov/quarterly-news/pdfs/odqnv1i2.pdf.

[82] NASA, Committee on Space Shuttle Meteoroid/Debris Risk Management, Protecting the Space Shuttle from Meteoroids and Orbital Debris (1997) at *V*.

[83] *Id.* at 16.

[84] Loretta Hall, *The History of Space Debris*, Space Traffic Management Conference, Embry-Riddle (Nov. 6, 2014), https://commons.erau.edu/cgi/viewcontent.cgi?article=1000&context=stm, at 3.

[85] Protecting the Space Shuttle, *supra* note 82, at 9.

[86] *Id.* at 15.

[87] Elizabeth Howell, *International Space Station: Facts, History & Tracking*, Space.com (Feb. 8, 2018), https://www.space.com/16748-international-space-station.html.

[88] Liou, *supra* note 52, at 6. For a comprehensive review of such ISS debris avoidance maneuvers, *see* James S. Cooney, *International Space Station (ISS) Orbital Debris Collision Avoidance Process*, NASA (Oct. 2016), https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20160012726.pdf.

[89] *See generally* Kessler & Cour-Palais, *supra* note 5.

[90] *Id.* at 2643. *See also* Antonio Lira, *How Long Does it Take for a Satellite to Fall to Earth?*, 50:1 Physics Educ. 71 (2015).

[91] Lira, *supra* note 90, at 73-74.

[92] IADC, IADC-15-03, *IADC Statement on Large Constellations in Low Earth Orbit* (Sept. 2017) at 6. For a comparison of the timelines for orbital decay at 400, 600, 800, and 1000 kilometers, see *Active Debris Removal*, *supra* note 20, at 18.

[93] *Towards Long-Term Sustainability*, *supra* note 51, at 21.

[94] Alexander F. Cohen, *Cosmos 954 and the International Law of Satellite Accidents*, 10:1 Yale J. Int'l L. 78, 79 (1984); W.K. Gummer et al., *COSMOS 954: The Occurrence and Nature of Recovered Debris*, 27 (May 1980), https://inis.iaea.org/collection/NCLCollectionStore/_Public/12/595/12595268.pdf?r=1&r=1.

[95] *Monthly Object Type Charts by Number and Mass*, *supra* note 7, at 10. It is important to note that the overall quantity of space objects increased relatively little, only 4%, between 2010 and 2018. However, because of the enormous NewSpace constellations planned for LEO in the near future (discussed in *infra* Part I(D)(4), and with some already having begun to launch), this recent pause in catalogued space object growth is unlikely to continue.

[96] *Monthly Object Type Charts by Number and Mass*, *supra* note 7, at 11.

[97] Ajey Lele, *The Implications of India's ASAT Test*, Space Rev. (Apr. 1, 2019), http://www.thespacereview.com/article/3686/1. The four countries are the U.S., the Soviet Union/Russia, China, and India.

[98] Joseph N. Pelton, New Solutions for the Space Debris Problem 3 (2015).

[99] T.S. Kelso, *Chinese ASAT Test*, CelesTrak (last updated June 22, 2012), https://celestrak.com/events/asat.php.

[100] Brian Weeden, *2007 Chinese Anti-Satellite Test Fact Sheet*, Secure World Foundation (last updated Nov. 23, 2010), https://swfound.org/media/9550/chinese_asat_fact_sheet_updated_2012.pdf, at 2.

[101] *Chinese Debris Reaches New Milestone*, 14:4 Orbital Debris Q. News 3, (Oct. 2010), https://www.orbitaldebris.jsc.nasa.gov/quarterly-news/pdfs/odqnv14i4.pdf.

[102] Brian Berger, *NASA's Tera Satellite Moved to Avoid Chinese ASAT Debris*, Space.com (July 6, 2007), https://www.space.com/4038-nasa-terra-satellite-moved-avoid-chinese-asat-debris.html; *Increase in ISS Debris Avoidance Maneuvers*, 16:2 Orbital Debris Q. News 1, 2, (Apr. 2012), https://orbitaldebris.jsc.nasa.gov/quarterly-news/pdfs/odqnv16i2.pdf.

[103] Weeden, *supra* note 100, at 3. It is important to note that these predictions were made in 2012 and can be influenced by a number of factors, especially solar radiation. *See Active Debris Removal, supra* note 20, at 18.

[104] *Id*.

[105] Brian Weeden, *2009 Iridium-Cosmos Collision Fact Sheet* 1, Secure World Foundation (last updated Nov. 10, 2010), https://swfound.org/media/6575/swf_iridium_cosmos_collision_fact_sheet_updated_2012.pdf.

[106] *Id*.

[107] T.S. Kelso, *Analysis of the Iridium 33-Cosmos 2251 Collision* 8, 10th Advanced Maui Optical and Space Surveillance Technologies Conference, Amos Tech (2009), https://amostech.com/TechnicalPapers/2009/Iridium_Cosmos_Collision/Kelso.pdf.

[108] P. Anz-Meador, *Top Ten Satellite Breakups Reevaluated*, 20:1-2 Orbital Debris Q. News 5, 6, (Apr. 2016), https://orbitaldebris.jsc.nasa.gov/quarterly-news/pdfs/odqnv20i1-2.pdf.

[109] Weeden, *supra* note 105, at 1.

[110] Ram S. Jahku, *Iridium-Cosmos Collision and Its Implications for Space Operations*, *in* Yearbook on Space Policy 2008/2009: Starting New Trends 263 (Kai-Uwe Schrogl et al., eds., 3d ed. 2010).

[111] *United Nations' COPUOS Receives Update on Iridium-Cosmos Collision*, 13:3 Orbital Debris Q. News 2, (July 2009), https://orbitaldebris.jsc.nasa.gov/quarterly-news/pdfs/odqnv13i3.pdf.

[112] *Chinese Debris Reaches New Milestone*, *supra* note 101.

[113] Kelso, *supra* note 107, at 7-8; *United Nations' COPUOS Receives Update on Iridium-Cosmos Collision*, *supra* note 111.

[114] *Top Ten Satellite Breakups Reevaluated*, *supra* note 108, at 6.

[115] Marco Langbroek, *Why India's ASAT Test Was Reckless*, Diplomat, (Apr. 30, 2019), https://thediplomat.com/2019/05/why-indias-asat-test-was-reckless/.

[116] Kerry Hebden, *Debris from India's ASAT Test Worse Than Predicated*, Room, (May 3, 2019), https://room.eu.com/news/debris-from-indias-asat-test-worse-than-predicted.

[117] Langbroek, *supra* note 115.

[118] *Id.*

[119] It is also worth noting the fact that, while many States expressed concern over this test and those before it, few, if any, declared such intentional debris-creating events to violate international space law, whether under Article IX of the OST, which contains "due regard," "harmful contamination," and "harmful interference" provisions, or any other provisions of international law. *See, for example,* Matteo Frigoli, *Between Active Debris Removal and Space-Based Weapons: A Comprehensive Legal Approach*, *in* Annette Froehlich, ed, Space Security and the Legal Aspects of Active Debris Removal 64 (Annette Froehlich ed., 2019); Jessica West, *It's Time to Speak Out About India's Reckless Anti-Satellite Test*, The Space Review (Apr. 15, 2019), https://www.thespacereview.com/article/3695/1. Interestingly, while the U.S. did not decry India's ASAT test as illegal, NASA Administrator Jim Bridenstine did state that the test was "unacceptable" and "a terrible, terrible thing …". *See* Brian Weeden, *India's ASAT Test is Wake-Up Call for Norms of Behavior in Space*, Space News (Apr. 8, 2019), https://spacenews.com/op-ed-indias-asat-test-is-wake-up-call-for-norms-of-behavior-in-space/. Some States even seemed to justify these events under the law. For example, after the Chinese ASAT test in 2007, a spokesman for the UK Prime Minister went so far as to say that the UK did not believe the test "contravene[d] international law." *See* Pavle Kilibarda, *The Militarization of Outer Space and the Liability Convention*, 40:3 Air & Space L. 271, 273 (2015).

[120] These countries include the UK, Canada, Italy, France, Australia, and West Germany, in that order. *See First Time in History*, The Satellite Encyclopedia (Mar. 3, 2019), https://www.tbs-satellite.com/tse/online/thema_first.html.

[121] Org. for Econ. Cooperation & Dev't (OECD), *The Space Economy at a Glance 2011*, 20 (2011), http://dx.doi.org/10.1787/9789264111790-en.

[122] T.S. Kelso, *SATCAT Sources*, CelesTrak, https://www.celestrak.com/satcat/sources.php (last visited Oct. 5, 2020).

[123] OECD, *supra* note 121, at 10.

[124] U.S., Fed. Aviation Admin. (FAA), T*he Annual Compendium of Commercial Space Transportation: 2018*, 1 (Jan. 2018), https://www.faa.gov/about/office_org/headquarters_offices/ast/media/2018_ast_compendium.pdf. For a detailed breakdown of the space economy from the same source, *see id.* at 9.

[125] FAA, *Licensed Launches*, https://www.faa.gov/data_research/commercial_space_data/launches/?type=license (last visited Oct. 6, 2020), *cf.* Jeff Foust, *SpaceX Launches Starlink Satellites as It Deorbits Original Ones*, SpaceNews, (Oct. 6, 2020), https://spacenews.com/spacex-launches-starlink-satellites-as-it-deorbits-original-ones/.

[126] Geoff Nunn, *Thinking Historically About NewSpace*, SpaceNews, (May 4, 2018), https://spacenews. com/op-ed-thinking-historically-about-newspace/; Bohumil Dobos & Jakub Prazak, *To Clear or to Eliminate? Active Debris Removal Systems as Antisatellite Weapons*, 47 Space Pol'y 217, 218 (2019).

[127] Jean-Marie Bockel, *The Future of the Space Industry: General Report*, North Atlantic Treaty Organization, Economic and Security Committee, 173 ESC 18 E fin (Nov. 17, 2018), https://www.nato-pa.int/document/2018-future-space-industry-bockel-report-173-esc-18-e-fin, at 2.

[128] Jeff Foust, *A Trillion Dollar Space Industry Will Require New Markets*, SpaceNews, (July 5, 2018), https://spacenews.com/a-trillion-dollar-space-industry-will-require-new-markets/.

[129] Caleb Henry, *OneWeb's First Six Satellites in Orbit Following Soyuz Launch*, SpaceNews, (Feb. 27, 2019), https://spacenews.com/first-six-oneweb-satellites-launch-on-soyuz-rocket/.

[130] Alan Boyle, *Amazon to Offer Broadband Access Form Orbit With 3,236-Satellite 'Project Kuiper' Constellation*, GeekWire (Apr. 4, 2019), https://www.geekwire.com/2019/amazon-project-kuiper-broadband-satellite/.

[131] Caleb Henry, *SpaceX Submits Paperwork for 30,000 More Starlink Satellites*, SpaceNews (Oct. 15, 2019), https://spacenews.com/spacex-submits-paperwork-for-30000-more-starlink-satellites/. As of February 2021, there are already well over 1,000 Starlink satellites in orbit, which have typically been launched in groups of 60. *See* Jeff Foust, *Falcon 9 Launches Starlink Satellites*, SpaceNews (Feb. 4, 2021), https://spacenews.com/falcon-9-launches-starlink-satellites/.

[132] Bockel, *supra* note 127, at 5.

[133] Between the 1950s and 2018, the estimated cost of launching one kilogram of mass into LEO decreased from nearly $1M USD to an incredible $1,400 USD. See Harry W. Jones, *The Recent Large Reduction in Space Launch Cost*, 48th Int'l Conf. on Envtl. Sys., (July 8-12, 2018), https://ttu-ir.tdl.org/bitstream/handle/2346/74082/ICES_2018%20_81.pdf?sequence=1&isAllowed=y

[134] Ellen Barry, *India Launches 104 Satellites From a Single Rocket, Ramping Up a Space Race*, N.Y. Times, (Feb. 15, 2017), https://www.nytimes.com/2017/02/15/world/asia/india-satellites-rocket.html. This record was recently shattered by SpaceX in January 2021 when the company successfully carried 143 satellites into orbit with a single launch. *See* Jeff Foust, *SpaceX Launches Record-Setting Cluster of Smallsats*, SpaceNews (Jan. 24, 2021), https://spacenews.com/spacex-launches-record-setting-cluster-of-smallsats/.

[135] Mark Garcia, *Space Debris and Human Spacecraft*, NASA, http://www.nasa.gov/mission_pages/station/news/orbital_debris.html (last updated Aug. 7, 2017).

[136] Henry T. Scott, *Improving the Shield: Mitigating the Danger of Space Debris by Enforcing and Developing Already Existing Space Law*, 34 Annals Air & Space L. 713, 723 (2009).

[137] M.Y.S. Prasad, *Technical and Legal Issues Surrounding Space Debris – India's Position in the UN,* 21 Space Pol'y 243, 244 (2005).

[138] Lyall & Larsen, *supra* note 15, at 276.

[139] NASA Safety Standard (NSS) 1740.14, *Guidelines and Assessment Procedures for Limiting Orbital Debris*, NASA (Aug. 1995), https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/19960020946.pdf. Several years earlier, in 1988, ESA had developed safety standard PSS-01-40, which, while not specifically devoted to space debris mitigation, contained basic requirements such as passivation that appear in most future mitigation guidelines. *See generally* Christophe Bonnal, Centre National d'Études Spatiales (CNES), Remarks at Clean Space Industrial Days: A Brief Historical Overview of Space Debris Mitigation Rules (May 23, 2016), https://indico.esa.int/event/128/attachments/729/798/01_Debris_Mitigation_-_Clean_Space_-_230516.pdf, at 7.

[140] NSS 1740.14, *supra* note 139, at 1-1.

[141] *Id.* For a detailed overview of this original debris mitigation standard, see generally Robert Reynolds et al., *An Overview of Revised NASA Safety Standard 1740.14*, Proc. 2d Eur. Conf. on Space Debris, SP-393, 721-726, (1996), https://conference.sdo.esoc.esa.int/proceedings/sdc2/paper/6/SDC2-paper6.pdf.

[142] Nat'l Res. Council, *Orbital Debris: A Technical Assessment*, NASA (1995), https://www.orbitaldebris.jsc.nasa.gov/library/a-technical-assessment.pdf; U.S., Nat'l Science & Tech. Council, *Interagency Report on Orbital Debris*, NASA (1995), https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20000011871.pdf.

[143] Scott, *supra* note 136, at 724.

[144] U.S., *Orbital Debris Mitigation Standard Practices*, NASA (1997), https://orbitaldebris.jsc.nasa.gov/library/usg_od_standard_practices.pdf [since being cited, this link appears to no longer be available].

[145] *Id.*

[146] Japan, Nat'l Space Dev't Agency of Japan, *Space Debris Mitigation Standard*, NASDA-STD-18 (Mar. 28, 1996).

[147] A. Kato, *Comparison of National Space Debris Mitigation Standards*, 28:9 Advances in Space Res. 1447, 1448-1449 (2001).

[148] France, CNES, RNC-CNES-Q40-512, CNES Standards Collection, Method and Procedure Space Debris – Safety Requirements (1999).

[149] Jinyuan Su, *Control Over Activities Harmful to the Environment*, *in* Routledge Handbook of Space Law 78 (Ram S. Jakhu & Paul Stephen Dempsey, eds., 2017).

[150] Russia, Russian Aviation and Space Agency, *Space Technology Items. General Requirements. Mitigation of Space Debris*, Standard OCT 134-1023 (2000).

[151] For a current list, *see* U.N. Office of Outer Space Affairs, *Compendium of Space Debris Mitigation Standards Adopted by States and International Organizations*, UNOOSA, http://www.unoosa.org/oosa/en/ourwork/topics/space-debris/compendium.html (last visited Oct. 6, 2020).

[152] Su, *supra* note 149, at 77.

[153] Karl-Heinz Böckstiegel, *ILA Draft Convention on Space Debris*, 43 Zeitschrift für Luft – und Weltraumrecht 395 (1994).

[154] Lotta Viikari, *Environmental Aspects of Space Activities*, *in* Handbook of Space Law 754 (Frans von der Dunk & Fabio Tronchetti eds., 2015).

[155] *Id.*

[156] Jan Wouters et al., Working Paper No. 153: *Space Debris Remediation, Its Regulation and the Role of Europe* 10, Ku Leuven (Mar. 2015), https://ghum.kuleuven.be/ggs/publications/working_papers/2015/153woutersdemanhansen.

[157] *European Code of Conduct for Space Debris Mitigation,* Issue 1.0, UNOOSA (June 28, 2004), http://www.unoosa.org/documents/pdf/spacelaw/sd/2004-B5-10.pdf. The other major national space agencies were from Italy, Germany, France, and the UK.

[158] Wouters et al., *supra* note 156, at 11; Viikari, *supra* note 154, at 751 n.171.

[159] *International Code of Conduct for Outer Space Activities*, draft version, European External Action Service (Mar. 31, 2014), https://eeas.europa.eu/sites/eeas/files/space_code_conduct_draft_vers_31-march-2014_en.pdf; Viikari, *supra* note 154, at 759-760.

[160] *International Code of Conduct*, *supra* note 159, art. 4(2).

[161] Viikari, *supra* note 154, at 760. *See also* Jinyuan Su & Zhu Lixin, *The European Union Draft Code of Conduct for Outer Space Activities: An Appraisal*, 30:1 Space Pol'y 34, 35 (2014).

[162] Cordula Steinkogler, *Small Satellites and Space Debris Mitigation*, *in* Small Satellites: Regulatory Challenge and Chances 225 (Irmgard Marboe ed., 2016).

[163] *Id.* at 225; Viikari, *supra* note 154, at 756.

[164] ESA, ESA/ADMIN/IPOL(2014)2, Space Debris Mitigation Policy for Agency Projects, IADC (Mar. 28, 2014), https://www.iadc-home.org/documents_public/file_down/id/4150 at 1.

[165] Steinkogler, *supra* note 162, at 223.

[166] ITU, Recommendation ITU-R S.1003-2, *Environmental Protection of the Geostationary-Satellite Orbit*, UNOOSA (2010), http://www.unoosa.org/documents/pdf/spacelaw/sd/R-REC-S1003-2-201012-IPDF-E.pdf.

[167] *Id.* at 1.

[168] Steinkogler, *supra* note 162, at 224.

[169] IADC-93-01, rev.11.5, *Terms of Reference for the IADC*, IADC (Oct. 3, 2018), https://www.iadc-home.org/terms_reference, at 3.

[170] *Space Debris Mitigation Guidelines*, *supra* note 20, at 3.

[171] *Id.*

[172] IADC, https://www.iadc-home.org/ (last visited Oct. 6, 2020).

[173] *Space Debris Mitigation Guidelines*, *supra* note 20, at 3; *Terms of Reference*, *supra* note 169, at 3.

[174] Lyall & Larsen, *supra* note 15, at 276.

[175] Steven A. Mirmina, *Reducing the Proliferation of Orbital Debris: Alternatives to a Legally Binding Instrument*, 99:3 Am. J. Int'l. L. 649, 661 (2005).

[176] Viikari, *supra* note 154, at 751. For a more thorough description of compliance with the IADC and other guidelines by state, see *Towards Long-Term Sustainability, supra* note 51, at 30-34.

[177] *Space Debris Mitigation Guidelines*, *supra* note 20, ¶ 1.

[178] *Id.* ¶¶ 1, 5.

[179] *Id.* ¶¶ 2, 3.5.

[180] *Id.* ¶ 3.1.

[181] *Id.* ¶ 3.3.2.

[182] *Id.* ¶ 4.

[183] *Id.* ¶ 5.1.

[184] *Id.* The term "acceptably low" is left undefined.

[185] *Id.* ¶ 5.2.1.

[186] *Id.* ¶ 5.2(3). The term "long-lived" is left undefined.

[187] *Id.* ¶ 5.3.1.

[188] *Id.* ¶ 5.3.2.

[189] *Id.* ¶ 5.4.

[190] Viikari, *supra* note 154, at 751; Su, *supra* note 149, at 77.

[191] *See generally* IADC, IADC-04-06, Rev 5.7, *Support to the IADC Space Debris Mitigation Guidelines* (May 2020), https://www.iadc-home.org/documents_public/file_down/id/4224.

[192] Comm. on the Peaceful Uses of Outer Space, Sci. and Tech. Subcomm., Technical Rep. on Space Debris, at 42, U.N. Doc. A/AC.105/720 (1999).

[193] The COPUOS Guidelines were adopted by the STSC in 2007. Comm. on the Peaceful Uses of Outer Space, Rep. of the Scientific and Technical Subcomm. on Its Forty-Fourth Session, at ¶ 99 & Annex IV, U.N. Doc. A/AC.105/890 (2007). They were thereafter endorsed by COPUOS. U.N. Doc. A/62/20, *supra* note 20, at ¶ 118 & Annex. UNOOSA helpfully maintains a stand-alone version of the COPUOS Guidelines. *Space Debris Mitigation Guidelines of the Committee on the Peaceful Uses of Outer Space,* UNOOSA (2007), http://www.unoosa.org/documents/pdf/spacelaw/sd/COPUOS-GuidelinesE.pdf.

[194] *See* UNGA Res 62/217, *supra* note 20, ¶¶ 26-27.

[195] Wouters et al., *supra* note 156, at 7.

[196] *See generally Space Debris Mitigation Guidelines*, *supra* note 193.

[197] Viikari, *supra* note 154, at 750.

[198] *Space Debris Mitigation Guidelines*, *supra* note 193, ¶ 4(7).

[199] *Id.* ¶ 4(6).

[200] *Id.* ¶ 3.

[201] Stephan Hobe & Jan Helge Mey, *UN Space Debris Mitigation Guidelines*, *in* International Space Law 631 (Frans G. von der Dunk ed., 2018); *Towards Long-Term Sustainability, supra* note 51, at 28.

[202] *See generally* Ram Jakhu, *The Effect of Globalisation on Space Law*, *in* Stephan Hobe, Globalisation – The State and International Law 74 (2009); *Towards Long-Term Sustainability, supra* note 51, at 29-30.

[203] Viikari, *supra* note 154, at 762.

[204] Comm. On the Peaceful Uses of Outer Space, *Guidelines for the Long-Term Sustainability of Outer Space Activities*, U.N. Doc. A/AC.105/208/CRP.20 (2018).

[205] *Annual Space Environment Report*, *supra* note 24, at 47.

[206] *Space Debris Mitigation Guidelines*, *supra* note 193, ¶ 3; *Space Debris Mitigation Guidelines*, *supra* note 20, ¶ 2.

[207] *Id*.

[208] Estoppel complaints for State violations would be unlikely to succeed since the COPUOS Guidelines expressly recognize at paragraph 3 that "exceptions to the implementation of individual guidelines or the elements thereof may be justified …."

[209] Scott, *supra* note 136, at 726.

[210] Su, *supra* note 149, at 77.

[211] *Towards Long-Term Sustainability, supra* note 51, at 37. *See also* Scott J. Shackelford, *Governing the Final Frontier: A Polycentric Approach to Managing Space Weaponization and Debris*, 51 Am. Bus. L.J. 429, 443 (2014).

[212] Cenan Al-Ekabi, *Reigniting Europe's Leadership in Debris Mitigation Efforts*, Open Access Government (May 24, 2018), https://www.openaccessgovernment.org/reigniting-europes-leadership-in-debris-mitigation-efforts/46074/.

[213] Hobe & Mey, *supra* note 201, at 629; *Space Debris Mitigation Guidelines*, *supra* note 193, at ¶ 3; IADC, *Space Debris Mitigation Guidelines*, *supra* note 20, ¶ 2.

[214] *Id*.

[215] Viikari, *supra* note 154, at 757.

[216] *Vanguard 1,* NASA, https://nssdc.gsfc.nasa.gov/nmc/spacecraft/display.action?id=1958-002B (last visited Oct. 6, 2020).

[217] *Active Debris Removal, supra* note 20, at 17; *See also* History of On-Orbit Satellite Fragmentations, *supra* note 21, at 3, fig.1.0-2.

[218] *Space Debris Mitigation Guidelines*, *supra* note 193, ¶ 4(4); *Space Debris Mitigation Guidelines*, *supra* note 20, ¶ 5.2(3).

[219] *Space Debris Mitigation Guidelines*, *supra* note 20, ¶ 5.3.2.

[220] *Id.* ¶ 5.2.3; *Space Debris Mitigation Guidelines*, *supra* note 193, ¶ 4(4).

[221] Su, *supra* note 149, at 77.

[222] *Space Environment Statistics, supra* note 1.

[223] *Towards Long-Term Sustainability, supra* note 51, at 30.

[224] Al-Ekabi, *supra* note 212.

[225] *Id.* at 35. For a discussion of MEO end-of-life strategies, see generally Raul Dominguez-Gonzalez et al., *Long-Term Implications of GNSS Disposal Strategies for the Space Debris Environment*, Proc. 7th Eur. Conf. on Space Debris, SDC-7, Eur. Space Agency (2017), https://conference.sdo.esoc.esa.int/proceedings/sdc7/paper/758/SDC7-paper758.pdf.

[226] The IADC Guidelines alone were drafted and agreed to by ESA and the space agencies of China, Japan, Russia, France, Germany, Italy, India, the U.S., and the U.K.. These countries, along with those represented by ESA, together account for an overwhelming majority of today's space activity. *See* Kelso, *SATCAT Boxscore*, *supra* note 2.

[227] *Annual Space Environment Report*, *supra* note 24, at 60. Note, however, that in compiling this data, ESA considers LEO re-orbits to altitudes above the protected region to be compliant with the IADC Guidelines, despite expressly stating at 56-57 that it is "against the spirit of those measures to leave space debris in orbit."

[228] *Id.* at 63.

[229] *Id.* at 64.

[230] Vincent Morand et al., *Mitigation Rules Compliance in Low Earth Orbit*, 1:2 J. Space Safety Eng'g 84, 89 (2014).

[231] *Id*.

[232] *Id.* at 91.

[233] *Annual Space Environment Report*, *supra* note 24, at 63.

[234] *Id.* at 65.

[235] *Id.* at 64.

[236] *Id.* at 63.

[237] Morand, *supra* note 230, at 91.

[238] *Annual Space Environment Report*, *supra* note 24, at 77.

[239] Mitsuru Ohnishi, *Review of IADC's Annual Activities* 13, IADC (2018), https://safe.menlosecurity.com/doc/docview/viewer/docNE3669FC83BDF4fde29619b5eef1e-2638b364023055704abc68fc81ff0685714713373049545c.

[240] *Annual Space Environment Report*, *supra* note 24, at 74.

[241] *Id*.

[242] *Towards Long-Term Sustainability, supra* note 51, at 35.

[243] *Annual Space Environment Report*, *supra* note 24, at 74.

[244] Ohnishi, *supra* note 239, at 13.

[245] Rong Du, *China's Approach to Space Sustainability: Legal and Policy Analysis*, 42 Space Pol'y 8, 9-10 (2017).

[246] Jim Wolf, *U.S. Shot Raises Tension and Worries Over Satellites*, Reuters (February 21, 2008), https://www.reuters.com/article/us-satellite-intercept-vulnerability/u-s-shot-raises-tensions-and-worries-over-satellites-idUSN2144210520080222; Kiona N. Smith, *India's Anti-Satellite Missile Test Left a Cloud of Debris and Tension in its Wake*, Forbes (April 5, 2019), https://www.forbes.com/sites/kionasmith/2019/04/05/indias-anti-satellite-missile-test-left-a-cloud-of-debris-and-tension-in-its-wake/#3ba9ae648fd1.

[247] *See supra* Part I, Sections D(1) and D(3); *see also*, Scott, *supra* note 136, at 730-734.

[248] *Space Debris Mitigation Guidelines*, *supra* note 193, ¶ 4(4); *Space Debris Mitigation Guidelines*, *supra* note 20, ¶ 5.2.3. It is worth noting that the United States' 2008 kinetic destruction of its own satellite (USA-193) was conducted at the relatively low altitude of about 250 kilometers and that the resultant debris field completely reentered within 18 months. The United States denied that this operation was in response to China's ASAT test and instead posited that it was necessary to protect the surface of the Earth from on-board, hazardous chemicals which could be released during an unguided reentry. *See* Stephen Clark, *U.S. Military Sensors Track Debris From Indian Anti-Satellite Test*, Spaceflight Now (Mar. 27, 2019), https://spaceflightnow.com/2019/03/27/u-s-military-sensors-track-debris-from-indian-anti-satellite-test/; *US Missile Hits 'Toxic Satellite,'* BBC (Feb. 21, 2008), http://news.bbc.co.uk/2/hi/americas/7254540.stm.

[249] *Monthly Object Type Charts by Number and Mass*, *supra* note 7, at 11.

[250] *Monthly Object Type Charts by Number and Mass*, *supra* note 7, at 10.

[251] Kelso, *SATCAT Boxscore*, *supra* note 2.

[252] *Monthly Object Type Charts by Number and Mass*, *supra* note 7, at 10.

[253] *Towards Long-Term Sustainability, supra* note 51, at 29.

[254] B. Bastida Virgili & H. Krag, Conf. Paper AAS 11-411, *Analyzing the Criteria for a Stable Environment* 1, AAS/AIAA Astrodynamics Specialist Conf. (2011), https://www.researchgate.net/publication/266556917_Analyzing_the_criteria_for_a_stable_environment.

[255] J.-C. Liou et al. *Controlling the Growth of Future LEO Debris Populations with Active Debris Removal*, 66:5-6 Acta Astronautica 648, 650 (2010).

[256] J.-C. Liou & N.L. Johnson, *Risks in Space From Orbiting Debris*, 311 Sci. 340 (2006).

[257] Virgili & Krag, *supra* note 254, at 12.

[258] Joseph N. Pelton, *Possible Institutional and Financial Arrangements for Active Removal of Orbital Debris*, *in* Handbook of Cosmic Hazards and Planetary Defense 854-855 (Joseph N. Pelton & Firooz Allahdadi eds., 2015). For a comparison of the growth of objects greater than 10 centimeters in LEO at current launch rates with 90% post-mission disposal alone, versus combined with ADR of either two or five objects per year, beginning in 2020, *see* J.-C. Liou, *NASA Orbital Debris Program Office Overview* 21, NASA (Mar. 2019), https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20190001584.pdf.

[259] *Id.*; Liou & Johnson, *supra* note 256, at 340.

[260] *Id*.

[261] *Stability of the Future LEO Environment*, *supra* note 67, at 17.

[262] *Id*. These space agencies included ASI, ESA, ISRO, JAXA, NASA, and UKSA.

[263] U.S., Space Policy Directive 3, National Space Traffic Management Policy ¶ 5(a)(3) (2018) [hereinafter SPD-3].

[264] Lyall & Larsen, *supra* note 15, at 280.

[265] Virgili & Krag, *supra* note 254, at 12.

[266] Peter Stubbe, State Accountability for Space Debris: A Legal Study of Responsibility for Polluting the Space Environment and Liability for Damage Caused by Space Debris 58-59 (2018).

[267] *See generally* C. Priyant Mark & Surekha Kamath, *Review of Active Debris Removal Methods*, 47 Space Pol'y 194 (2019).

[268] *Id.* at 204.

[269] *See, e.g.*, Pelton, *supra* note 98, at 11-26.

[270] Minghe Shan et al., *Review and Comparison of Active Space Debris Capturing and Removal Methods*, 80 Progress in Aerospace Sci. 18, 28 (2016).

[271] Akihiro Sasoh et al., *Characteristics of Ablation Impulse Induced by Repetitive Laser Impulse Radiations*, Proc. 7th Eur. Conf. on Space Debris, SP-672, 2, Eur. Space Agency (2017), https://conference.sdo.esoc.esa.int/proceedings/sdc7/paper/298/SDC7-paper298.pdf.

[272] Shan et al., *supra* note 270, at 28.

[273] Brian Weeden, *Overview of the Legal and Policy Challenges of Orbital Debris Removal*, 27:1 Space Pol'y 38, 39 (2011).

[274] Claude R. Phipps et al., *Removing Orbital Debris With Lasers* 3, arXiv.org (2011), https://arxiv.org/ftp/arxiv/papers/1110/1110.3835.pdf; Shan et al., *supra* note 270, at 28.

[275] Mark & Kamath, *supra* note 267, at 197.

[276] Quan Wen, *Removing Small Scale Space Debris by Using a Hybrid Ground and Space Based Laser System*, 141 Optik 105, 105 (2017).

[277] Pelton, *supra* note 98, at 55.

[278] Claude R. Phipps, *A Laser-Optical System to Re-Enter or Lower Low Earth Orbit Space Debris*, 93 Acta Astronautica 418, 419 (2014).

[279] *Id.*; Claude R. Phipps & Christophe Bonnal, *A Spaceborne, Pulsed UV Laser System for Re-Entering or Nudging LEO Debris, and Re-orbiting GEO Debris*, 118 Acta Astronautica 224, 227 (2016); Sasoh et al., *supra* note 271, at 2.

[280] *See generally* Michael Mercurio et al., *Debris-Laser Beam Probability of Intersection in the Presence of Uncertainty*, Proc. 7th Eur. Conf. on Space Debris, SDC-7, 4, Eur. Space Agency (2017), https://conference.sdo.esoc.esa.int/proceedings/sdc7/paper/174/SDC7-paper174.pdf; J.-C. Liou, *Active Debris Removal and the Challenges for Environment Remediation* 4, NASA (June 17, 2012), https://ntrs.nasa.gov/citations/20120013266.

[281] *See generally id*.; *see also* Pelton, *supra* note 98, at 41-42.

[282] Pelton, *supra* note 98, at 57-58.

[283] R. Benvenuto et al., *Tethered-Tugs for Active Debris Removal: Microgravity Experimental Validation of Dynamics and Control*, Proc. 7th Eur. Conf. on Space Debris, SDC-7, 1, Eur. Space Agency (2017), https://conference.sdo.esoc.esa.int/proceedings/sdc7/paper/725/SDC7-paper725.pdf.

[284] *See generally* Shan et al., *supra* note 270, at 19-25; Pelton, *supra* note 98, at 20; Umberto Battista et al., *Design of Net Ejector for Space Debris Capturing*, Proc. 7th Eur. Conf. on Space Debris, SDC-7, Eur. Space Agency (2017), https://conference.sdo.esoc.esa.int/proceedings/sdc7/paper/279/SDC7-paper279.pdf.

[285] *Id*.

[286] Pelton, *supra* note 98, at 58.

[287] *Id*.

[288] Shin-Ichiro Nishida et al., *Space Debris Removal System Using a Small Satellite*, 65 Acta Astronautica 95, 95-96 (2009).

[289] *Id.* at 101; Shan et al., *supra* note 270, at 29.

[290] Aleksander A. Lidtke et al., *Considering the Collision Probability of Active Debris Removal Missions*, 131 Acta Astronautica 10, 10 (2017); Nishida et al., *supra* note 288, at 95-96 & 101.

[291] Lidtke et al., *supra* note 290, at 10.

[292] Pelton, *supra* note 98, at 65.

[293] Patent No. U.S. 9,555,905 B2, *supra* note 16, at 8-10 & 31.

[294] Nishida et al., *supra* note 288, at 96; Shan et al., *supra* note 270, at 26-27.

[295] *Orbital Debris Management*, *supra* note 6, at 29; Shan et al., *supra* note 270, at 26-27; *see generally* Nishida et al., *supra* note 288.

[296] For a full overview of this project and its progress, *see* G.S. Aglietti et al., *RemoveDEBRIS Mission: 2nd Briefing to UN COPUOS*, Sci. & Tech. Subcomm., UNOOSA (Feb. 2019), http://www.unoosa.org/documents/pdf/copuos/stsc/2019/tech-32E.pdf.

[297] Shan et al., *supra* note 270, at 27; Aglietti, *supra* note 296, at 10.

[298] Aglietti, *supra* note 296, at 10.

[299] *See generally* Craig Underwood et al., *The InflateSail CubeSat Mission – The First European Demonstration of Drag-Sail De-Orbiting*," 4th IAA Conf. on Univ. Satellite Missions & CubeSat Workshop, IAA-AAS-CU-17-04-05, Univ. of Surrey (Dec. 2017), https://epubs.surrey.ac.uk/849323/1/The%20inflatesail%20cubesat%20mission.pdf.

[300] Pelton, *supra* note 98, at 59; Shan et al., *supra* note 270, at 26;

[301] Shan et al., *supra* note 270, at 26.

[302] Weeden, *supra* note 273, at 39-40.

[303] Pelton, *supra* note 98, at 55.

[304] *Active Debris Removal, supra* note 20, at 26.

[305] Joshua Tallis, *Remediating Space Debris*, 9:1 Strategic Stud. Q. 86, 89 (2015).

[306] C. Q. Christol, *Suggestions for Legal Measures and Instruments for Dealing with Debris*, *in* Environmental Aspects of Activities in Outer Space 257 (Karl-Heinz Böckstiegel ed., 1990).

[307] *Space Debris Mitigation Guidelines*, *supra* note 193, at para 1; *Space Debris Mitigation Guidelines*, *supra* note 20, ¶ 3.1.

[308] G.A. Res. 62/217, *supra* note 20, ¶¶ 26 & 27.

[309] Hobe & Mey, *supra* note 201, at 628.

[310] *Id*.

[311] Joyeeta Chatterjee et al., *Active Orbital Debris Removal and the Sustainability of Space*, *in* Handbook of Cosmic Hazards and Planetary Defense 935 (Joseph N. Pelton & Firooz Allahdadi eds., 2015).

[312] OST, *supra* note 10, art. IX.

[313] Ram S. Jakhu & Yaw O. M. Nyampong, *Some Legal and Regulatory Constraints on the Conduct of Removal and On-Orbit Satellite Servicing*, 63rd Int'l Astronautical Cong., IAC-12, A6, 6, 6, x13110 (2012), at 8; Pelton, *supra* note 98, at 6.

[314] Steinkogler, *supra* note 162, at 213; Bin Cheng, Studies in International Space Law (1997), at 506.

[315] Liability Convention, *supra* note 11, art. I(d); Registration Convention, *supra* note 13, art. I(b).

[316] Christol, *supra* note 306, at 259.

[317] Chatterjee, et al, *supra* note 311, at 935.

[318] Stephen Gorove, Developments in Space Law: Issues and Policies 165 (1991); Frigoli, *supra* note 119, at 54-55.

[319] Cheng, *supra* note 314, at 506; Jakhu & Nyampong, *supra* note 313, at 7; Steinkogler, *supra* note 162, at 213-214. *But see* Zhuang Tian, *Proposal for an International Agreement on Active Debris Removal*, *in* Space Security and the Legal Aspects of Active Debris Removal 118-120 (Annette Froehlich ed., 2019) for why some commentators disagree with this interpretation of the scope of "space objects."

[320] Pelton, *supra* note 98, at 74.

[321] Cheng, *supra* note 314, at 506.

[322] Chatterjee et al., *supra* note 311, at 935.

[323] Philip de Man, *Disused Unitary Satellites and the Non-Appropriation Principle: A Functional Comparison*, *in* Global Space Governance 453 (Ram Jakhu et al. eds., 2015).

[324] Tian, *supra* note 319, at 117; Alexander William Salter, *Space Debris: A Law and Economics Analysis of the Orbital Commons*, 19 Stan. Tech. L. Rev. 221, 233-234 (2016).

[325] Jakhu & Nyampong, *supra* note 313, at 7.

[326] Ram S. Jakhu et al., *Critical Issues Related to Registration of Space Objects and Transparency of Space Activities*, 143 Acta Astronautica 406, 410 (2018).

[327] *Id.* at 407.

[328] Registration Convention, *supra* note 13, art. IV(2).

[329] Darren McKnight & Kris Walbert, *Proposed Series of Orbital Debris Remediation Activities*, Proc. 7th Eur. Conf. on Space Debris, SDC-7, 2 Eur. Space Agency (2017), https://conference.sdo.esoc.esa.int/proceedings/sdc7/paper/1/SDC7-paper1.pdf; Weeden, *supra* note 273, at 40; *See generally* Jakhu et al., *supra* note 326.

[330] Jakhu et al., *supra* note 326, at 411 & 413-414.

[331] Weeden, *supra* note 273, at 40.

[332] Hobe & Mey, *supra* note 201, at 628.

[333] *Id*.

[334] Pelton, *supra* note 98, at 70.

[335] Wouters et al., *supra* note 156, at 6.

[336] Popova & Schaus, *supra* note 50, at 4.

[337] Wouters et al., *supra* note 156, at 6.

[338] N. Jasentuliyana, *Space Debris and International Law*, 26 J. Space L. 139, 141 (1998).

[339] *See* Wouters et al., *supra* note 156, at 7 for such a comparison.

[340] *Space Debris Mitigation Guidelines*, *supra* note 193, ¶ 4(4); *Space Debris Mitigation Guidelines*, *supra* note 20, ¶ 5.2.3.

[341] Wouters et al., *supra* note 156, at 7; Frigoli, *supra* note 119, at 64.

[342] Wouters et al., *supra* note 156, at 6.

[343] Du, *supra* note 245, at 11; Popova & Schaus, *supra* note 50, at 6; *Towards Long-Term Sustainability*, *supra* note 51, at 22-23; Ram S. Jakhu, *Regulatory Aspects Associated with Response to Man-Made Cosmic Hazards*, *in* Handbook of Cosmic Hazards and Planetary Defense 1072 (Joseph N. Pelton & Firooz Allahdadi eds., 2015); M. Emanuelli et al., *Conceptualizing an Economically, Legally, and Politically Viable Active Debris Removal Option*, 104 Acta Astronautica 197, 200 (2014).

[344] Peter Malanczuk, *Review of the Regulatory Regime Governing the Space Environment – The Problem of Space Debris*, 45 Zeitschrift für Luft- und Weltraumrecht 37, 58 (1996); Popova & Schaus, *supra* note 50, at 6.

[345] Pelton, *supra* note 98, at 33.

[346] OST, *supra* note 10, art. VIII.

[347] G.A. Res. 1962 (XVIII), *Declaration of Legal Principles Governing the Activities of States in the Exploration and Use of Outer Space*, U.N. Doc. A/RES/1962 (XVIII) (1963).

[348] *Id.* ¶ 7.

[349] OST, *supra* note 10, art. VIII. While the language in art. VIII is nearly identical to the 1963 UNGA Declaration, it expands the concept by also applying ownership to objects landed on or constructed on celestial bodies.

[350] Registration Convention, *supra* note 13, art. II(1).

[351] *Id.* art. II(2).

[352] *Id.* art. II(3).

[353] *Id.* arts. III & IV.

[354] *Id.* art. I(c).

[355] Popova & Schaus, *supra* note 50, at 9; Pelton, *supra* note 98, at 74; Gordon Chung, *Jurisdiction and Control Aspects of Space Debris Removal*, *in* Space Security and the Legal Aspects of Active Debris Removal 33-34 (Annette Froehlich ed., 2019).

[356] *Active Debris Removal, supra* note 20, at 32; OST, *supra* note 10, art. II; Chung, *supra* note 355, at 33; Frigoli, *supra* note 119, at 55.

[357] de Man, *supra* note 323, at 451.

[358] *Id.* at 452; Weeden, *supra* note 273, at 41; Frigoli, *supra* note 119, at 56; Popova & Schaus, *supra* note 50, at 9.

[359] Malanczuk, *supra* note 344, at 59; F. K. Schwetje, *Liability and Space Debris*, *in* Environmental Aspects of Activities in Outer Space 36-37 (Karl-Heinz Böckstiegel ed., 1990).

[360] Weeden, *supra* note 273, at 41; Pelton, *supra* note 98, at 74.

[361] For a thorough description of how such a target should be selected, including several identified targets, see Christophe Bonnal et al., *Space Debris Removal: Recent Progress and Current Trends*, 85 Acta Astronautica 51, 54-55 (2013).

[362] Weeden, *supra* note 273, at 41.

[363] *Id*.

[364] Jerome Pearson et al., *EDDE Spacecraft Development for Active LEO Debris Removal*, 65th Int'l Astronautical Cong., IAC-14, A6, 6.4x23806, Star-Tech, Inc. (2014), http://www.star-tech-inc.com/papers/EDDE_Debris_Paper_IAC14A664x-23806_2014Sept28.pdf, at 10 & 14.

[365] Popova & Schaus, *supra* note 50, at 9.

[366] *Active Debris Removal, supra* note 20, at 32; OST, *supra* note 10, art. VIII; Chung, *supra* note 355, at 38-41.

[367] Chatterjee et al., *supra* note 311, at 935.

[368] *Id.* at 936; Pelton, *supra* note 98, at 74.

[369] *See* Jakhu et al., *supra* note 326, at 412 for a description of this on-orbit transfer and three others, each resulting in varying levels of registration.

[370] *Id*.

[371] *Id.* at 413.

[372] G.A. Res. 59/115, *Application of the Concept of the "Launching State"* ¶¶ 3-4, U.N. Doc. A/RES/59/115 (2004).

[373] G.A. Res. 62/101, *Recommendations on Enhancing the Practice of States and International Intergovernmental Organizations in Registering Space Objects* ¶ 4(a), U.N. Doc. A/RES/62/101 (2007).

[374] *Id.* ¶ 4(b).

[375] Jakhu et al., *supra* note 326, at 412.

[376] Chatterjee et al., *supra* note 311, at 936.

[377] Lyall & Larsen, *supra* note 15, at 78; Malanczuk, *supra* note 344, at 59.

[378] *See* de Man, *supra* note 323, at 452-453 for several of these authors, including Bin Cheng and CW Jenks; *See also*, Chung, *supra* note 355, at 41; Chelsea Muñoz-Patchen, *Regulating the Space Commons: Treating Space Debris as Abandoned Property in Violation of the Outer Space Treaty*, 19:1 Chicago J. Int'l L. 233, 246-250 (2018).

[379] Frigoli, *supra* note 119, at 57.

[380] Hamilton DeSaussure, *An International Right to Reorbit Earth Threatening Satellites*, 3 Annals Air & Space L. 383, 391 (1978), stating, "Derelict property in maritime law is property on the high seas (or other navigable waters) which has been abandoned by those in charge of it without hope of recovering it or returning to it." Since such derelict property is legally salvageable by all States, it creates an interesting contrast with uncontrolled, abandoned space debris that remains under the jurisdiction and responsibility of its launching state. For an extensive discussion of this analogy, *see* Christol, *supra* note 306, at 268-276.

[381] Pelton, *supra* note 98, at 74; Tallis, *supra* note 305, at 91; Muñoz-Patchen, *supra* note 378, at 245.

[382] Jasentuliyana, *supra* note 338, at 144; R. Ghadawala et al., *Commercial Aspects of Active Debris Removal: Technical and Legal Challenges*, 5:1 J. Aeronautics & Aerospace Eng'g 1, 4 (2016).

[383] Jakhu et al., *supra* note 326, at 407.

[384] *Id.*; Lyall & Larsen, *supra* note 15, at 79; Agatha Akers, *To Infinity and Beyond: Orbital Space Debris and How to Clean It Up*, 33:2 U. La Verne L. Rev. 285, 306-207 (2012).

[385] Lyall & Larsen, *supra* note 15, at 78; Frigoli, *supra* note 119, at 58.

[386] Christol, *supra* note 306, at 268; Muñoz-Patchen, *supra* note 378, at 245-246; de Man, *supra* note 323, at 453.

[387] *Active Debris Removal, supra* note 20, at 32.

[388] Liability Convention, *supra* note 11, arts. II-III.

[389] Pelton, *supra* note 98, at 71.

[390] G.A. Res. 1962 (XVIII), *supra* note 347, ¶ 8.

[391] Liability Convention, *supra* note 11, art. I(c).

[392] OST, *supra* note 10, art. VII.

[393] Liability Convention, *supra* note 11, arts. II & III.

[394] *Id.* art. I(a). Note that this seriously limits the Liability Convention's application to environmental damage. *See* Lawrence D. Roberts, *Addressing the Problem of Orbital Space Debris: Combining International Regulatory and Liability Regimes*, 15 B.C. Int'l & Comp. L. Rev. 51, 64 (1992).

[395] Frigoli, *supra* note 119, at 57.

[396] Schwetje, *supra* note 359, at 40; Jasentuliyana, *supra* note 338, at 143.

[397] Liability Convention, *supra* note 11, art. I(c).

[398] Pelton, *supra* note 98, at 31.

[399] Stubbe, *supra* note 266, at 397-399.

[400] Liability Convention, *supra* note 11, art. V(1).

[401] *Id.* art. IV.

[402] *Id.* art. IV(2).

[403] Scott, *supra* note 136, at 746; Gorove, *supra* note 318, at 165. Note that some commentators maintain that a plain reading of the Liability Convention excludes fragments from the definition of "space objects." *See, e.g.*, Roberts, *supra* note 394, at 64 & Tian, *supra* note 319, at 118-120.

[404] History of On-Orbit Satellite Fragmentations, *supra* note 21, at 3.

[405] Weeden, *supra* note 273, at 41; Tian, *supra* note 319, at 125.

[406] Roberts, *supra* note 394, at 55.

[407] Nishida et al., *supra* note 288, at 95-96; Shan et al., *supra* note 270, at 29; Weeden, *supra* note 273, at 41.

[408] Shan et al., *supra* note 270, at 25.

[409] Jakhu et al., *supra* note 9, at 130.

[410] Phipps & Bonnal, *supra* note 279, at 227.

[411] Weeden, *supra* note 273, at 42.

[412] *Id.* at 41-42; *Active Debris Removal, supra* note 20, at 32.

[413] Weeden, *supra* note 273, at 41-42.

[414] Liability Convention, *supra* note 11, art. III.

[415] *Id.*

[416] Malanczuk, *supra* note 344, at 53-54; Shackelford, *supra* note 211, at 497; Stubbe, *supra* note 266, at 405-406.

[417] Scott Kerr, *Liability for Space Debris Collisions and the Kessler Syndrome (Part 1)*, Space Rev. (Dec. 11, 2017), http://www.thespacereview.com/article/3387/1. The only time the Liability Convention has been invoked since its inception almost 50 years ago was for damage caused in Canada from the reentry and crashing of the Soviet nuclear satellite Cosmos-954 in 1978. *See generally* Cohen, *supra* note 94.

[418] Registration Convention, *supra* note 13, art. II.

[419] Schwetje, *supra* note 359, at 40-41; Tallis, *supra* note 305, at 90.

[420] *Id.* at 40.

[421] Jasentuliyana, *supra* note 338, at 143; Tian, *supra* note 319, at 126.

[422] Kerr, *supra* note 417.

[423] Liability Convention, *supra* note 11, art. II.

[424] Popova & Schaus, *supra* note 50, at 10; Pelton, *supra* note 98, at 73-74.

[425] Jakhu et al., *supra* note 326, at 408.

[426] Pelton, *supra* note 98, at 71 & 73.

[427] *Id.* at 71 & 74-75.

[428] Babak Shakouri Hassanabadi, *Complications of the Legal Definition of 'Launching State'*, Space Rev. (Sept. 2, 2014), http://www.thespacereview.com/article/2588/1.

[429] *Id.*; Popova & Schaus, *supra* note 50, at 10.

[430] Popova & Schaus, *supra* note 50, at 10; Liability Convention, *supra* note 11, art. V.

[431] Pelton, *supra* note 98, at 73.

[432] Research Regulatory Affairs, *Export Control Definitions and Terms*, Rutgers Univ., https://orra.rutgers.edu/ecdefinitions (last visited Oct. 16, 2020).

[433] Fabio Tronchetti, *Legal Aspects of the Military Uses of Outer Space*, *in* Handbook of Space Law 367 (Frans von der Dunk & Fabio Tronchetti eds., 2015); 15 C.F.R. § 734.14.

[434] Stanley J. Marcuss & Michael B. Zara, *A Better Way Through the Export Control Thicket*, 14 Santa Clara J. Int'l L. 47, 48 (2016); 15 C.F.R. § 730.6.

[435] *Active Debris Removal, supra* note 20, at 34.

[436] *Id.*; 15 C.F.R. § 730.5; Tian, *supra* note 319, at 121-122. The United States generally defines the "export" of controlled objects as: (1) an actual shipment or transmission out of the U.S., (2) releasing or otherwise transferring technical data to a foreign person in the United States, (3) transferring registration, control, or ownership of any aircraft, vessel, or satellite by a U.S. person to a foreign person, (4) releasing or otherwise transferring a defense article to an embassy in the United States, or (5) performing a defense service on behalf of, or for the benefit of, a foreign person, whether in the United States or abroad. *See* 22 C.F.R. § 120.17; 15 C.F.R. § 734.13; U.S., Department of Commerce's Office of Space Commerce & Federal Aviation Administration's Office of Commercial Space Transportation, *Introduction to U.S. Export Controls for the Commercial Space Industry*, 2d ed., Office of Space Commerce (Nov. 2017), https://www.space.commerce.gov/wp-content/uploads/2017-export-controls-guidebook.pdf.

[437] Jakhu et al., *supra* note 9, at 131.

[438] Ram S. Jakhu, *Regulation of Space Activities in Canada*, *in* National Regulation of Space Activities 87-91 (Ram S. Jakhu ed., 2010); Global Affairs Canada, *A Guide to Canada's Export Controls*, Government of Canada, https://www.international.gc.ca/controls-controles/about-a_propos/expor/guide.aspx?lang=eng (last updated May 13, 2016).

[439] Philippe Achilleas, *Regulation of Space Activities in France*, *in* National Regulation of Space Activities 121 (Ram S. Jakhu ed., 2010).

[440] Ranjana Kaul & Ram S. Jakhu, *Regulation of Space Activities in India*, *in* National Regulation of Space Activities 166-169 & 196-197 (Ram S. Jakhu ed., 2010).

[441] *See generally* Vladamir A. Orlov, *Export Controls in Russia: Policies and Practices*, 6:4 Nonproliferation Rev. 139 (1999).

[442] Yun Zhao, *Regulation of Space Activities in the People's Republic of China*, *in* National Regulation of Space Activities 263-264 (Ram S. Jakhu ed., 2010).

[443] Jakhu et al., *supra* note 9, at 132.

[444] For an amusing explanation of the confusing and overlapping expanse of U.S. export control regulation, *see generally* Marcuss & Zara, *supra* note 434, where the authors describe the incomprehensible web of more than 1,500 pages of regulations spread across three federal agencies. Prior to 2014, the export-controlling U.S. Munitions List (USML), maintained by the Department of State (DoS), contained virtually all space-related technology. *Introduction to U.S. Export Controls*, *supra* note 436, at 5-6 & 8; 22 C.F.R. § 121.1. Items and covered technology on this list are considered "defense articles" without any civilian use and require a license prior to exporting or re-exporting them to any foreign person or State. Mark J. Sundahl, *Space Tourism and Export Controls: A Prayer for Relief*, 75 J. Air L. & Com. 581, 590 (2010); 22 C.F.R. § 120.6. In 2014, the DoS reorganized the USML to remove a significant amount of civil and commercial satellite technology. Bockel, *supra* note 127, at 4; *Introduction to U.S. Export Controls*, *supra* note 436, at 8-9. Still, certain critical technologies remain on the USML, such as various rocket and space launch vehicle technology under Category IV and various classified spacecraft and ground control systems under Category XV, including the components, technical data, and services of each of these. *Introduction to U.S. Export Controls*, *supra* note 436, at 21; 22 C.F.R. § 121.1. Notably, China, a major global space power, is categorically barred from exports under the current ITAR. 22 C.F.R. § 126.1(d)(1). Despite the loosening of these restrictions, most space technologies are still subject to export control through the Department of Commerce's Export Administration Regulations (EAR) and Commerce Control Lists (CCL), which operate to restrict the export of certain unclassified, dual-use goods and technologies, including but not limited to training simulators, production equipment, ISS equipment, and spacecraft buses. *Introduction to U.S. Export Controls*, *supra* note 436, at 1, 5-6, 8-9 & 25-29; 15 C.F.R. pt. 774. Notably, the EAR carves out export license exceptions for certain U.S. allies, primarily NATO countries. 15 C.F.R. § 740.20; *Introduction to U.S. Export Controls*, *supra* note 436, at 9-10.

[445] Bockel, *supra* note 127, at 4; Peter B. de Selding, *U.S. ITAR Satellite Export Regime's Effects Still Going Strong in Europe*, Space News, (Apr. 14, 2016), https://spacenews.com/u-s-itar-satellite-export-regimes-effects-still-strong-in-europe/.

[446] Caleb Henry, *Back-to-Back Commercial Satellite Wins Leave China Great Wall Hungry for More*, Space News, (Aug. 22, 2017), https://spacenews.com/back-to-back-commercial-satellite-wins-leave-china-great-wall-hungry-for-more/.

[447] Commission Delegated Regulation (E.U.) 2018/1922, amending Council Regulation (E.C.) No. 428/2009 *Setting up a Community Regime for the Control of Exports, Transfer, Brokering, and Transit of Dual-Use Items*, OJ L 319 (2018). For a detailed discussion of EU export controls, see Tronchetti, *supra* note 433, at 369-377.

[448] Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, Final Declaration 4, Wassenaar.org (Dec. 19, 1995), https://www.wassenaar.org/app/uploads/2015/06/WA-DOC-17-PUB-001-Public-Docs-Vol-I-Founding-Documents.pdf. The purpose of the Wassenaar Arrangement is to "promote transparency and greater responsibility in transfers of conventional and dual-use goods and technologies, thus preventing destabilizing accumulations." *Id.; See also*, Tronchetti, *supra* note 433, at 363-366.

[449] *See generally* Wassenaar Arrangement, *List of Dual-Use Goods and Technologies and Munitions List*, Wassenaar.org (Dec. 2018), https://www.wassenaar.org/app/uploads/2018/12/WA-DOC-18-PUB-001-Public-Docs-Vol-II-2018-List-of-DU-Goods-and-Technologies-and-Munitions-List-Dec-18.pdf. For an example of Wassenaar-controlled space technology, *see id.* ¶ 9.A.4.

[450] Pelton, *supra* note 98, at 6, 75-76; McKnight & Walbert, *supra* note 329, at 4.

[451] Pelton, *supra* note 98, at 76.

[452] U.S., Space Policy Directive 3, *supra* note 263, ¶ 5(c).

[453] Pelton, *supra* note 258, at 866-867; Jakhu et al., *supra* note 9, at 135-136.

[454] Pelton, *supra* note 98, at 76; *See also* Popova & Schaus, *supra* note 50, at 12.

[455] Carsten Weidemann et al., *The Economics of the Control of the Space Debris Environment*," Proc. 6th Eur. Conf. on Space Debris, SDC-6, Paper 86, 2, Eur. Space Agency (2013), https://conference.sdo.esoc.esa.int/proceedings/sdc6/paper/86/SDC6-paper86.pdf.

[456] Pelton, *supra* note 98, at 58.

[457] *Id.* at 25.

[458] *See generally* Toru Yamamoto et al., *Cost Analysis of Active Debris Removal Scenarios and System Architectures*, Proc. 7th Eur. Conf. on Space Debris, SDC-7, Paper 660, Eur. Space Agency (2017), https://conference.sdo.esoc.esa.int/proceedings/sdc7/paper/660/SDC7-paper660.pdf.

[459] McKnight & Walbert, *supra* note 329, at 4.

[460] *Id.* at 5.

[461] Leonard Vance & Allan Mense, *Value Analysis for Orbital Debris Removal*, 52 Advances in Space Res. 685, 692 & 694 (2013).

[462] Satomi Kawamoto et al., *Current Status of Research and Development on Active Debris Removal at JAXA*, Proc. 7th Eur. Conf. on Space Debris, SP-672, 1, Eur. Space Agency (2017), https://conference.sdo.esoc.esa.int/proceedings/sdc7/paper/655/SDC7-paper655.pdf.

[463] Kelso, *SATCAT Boxscore*, *supra* note 2.

[464] United Nations Framework Convention on Climate Change arts. 3(1) & 4(1), May 9, 1992, 1771 U.N.T.S. 107 [hereinafter UNFCCC].

[465] Weeden, *supra* note 273, at 42; Frigoli, *supra* note 119, at 62.

[466] Frigoli, *supra* note 119, at 60 & 62; Tallis, *supra* note 305, at 92-93.

[467] Frigoli, *supra* 119, at 62; Dobos & Prazak, *supra* note 126, at 221.

[468] Jakhu, s*upra* note 343, at 1072.

[469] Weeden, *supra* note 273, at 42. Such an outcry did, in fact, follow testing by China of on-orbit servicing and satellite capture technology in 2013. *See* Frigoli, *supra* note 119, at 67.

[470] Popova & Schaus, *supra* note 50, at 10.

[471] Tian, *supra* note 319, at 114-115.

[472] *Id.*; Mirmina, *supra* note 175, at 658.

[473] Christopher D. Williams, *Space: The Cluttered Frontier*, 60:4 J. Air L. & Com. 1139, 1182-1183 (1995).

[474] *Id.* at 1182.

[475] Liou, *supra* note 258, at 21.

[476] *See, e.g., Guidelines for the Long-Term Sustainability of Outer Space Activities*, *supra* note 204; UNGA Res 62/217, *supra* note 20.

[477] Tian, *supra* note 319, at 116-117.

[478] *Id.* at 117.

[479] History of On-Orbit Satellite Fragmentations, *supra* note 21, at 3.

[480] Tian, *supra* note 319, at 118-119.

[481] *Id.*; Frigoli, *supra* 119, at 55; Gorove, *supra* note 318, at 165.

[482] Williams, *supra* note 473, at 1184-1185.

[483] *Top Ten Satellite Breakups Reevaluated*, *supra* note 108, at 6.

[484] *E.g.*, the Partial Nuclear Test Ban Treaty of 1963 banned nuclear tests in the atmosphere, outer space, and underwater. *See generally* Treaty Banning Nuclear Weapon Tests in the Atmosphere, in Outer Space and Under Water, Aug. 5 1963, 14 U.S.T. 1313, 480 U.N.T.S. 43 [hereinafter PTBT].

[485] *Active Debris Removal*, supra note 20, at 40.

[486] Liou, *supra* note 258, at 21.

[487] Tian, *supra* note 319, at 127; *Active Debris Removal*, supra note 20, at 32.

[488] Liability Convention, *supra* note 11, art. IV.

[489] Jakhu et al., *supra* note 9, at 132.

[490] *Id.* at 132.

[491] Cheng, *supra* note 314, at 506-507.

[492] *Id.* at 506.

[493] Pelton, *supra* note 98, at 44. Jakhu, Nyampong, and Sgobba have called for an organization mirroring INTELSAT, which they described as a "group of public and private joint venturers, combining their technical and financial resources to establish and operate facilities which each participant intended to use to provide services within its defined market area." They propose creating a multinational ADR organization via a state-driven treaty document outlining the scope and structure of the organization itself and an additional operating agreement which outlines the rights and obligations of its members, which they believe should include private and public space industry operators. *See generally* Jakhu et al., *supra* note 9.

[494] Akers, *supra* note 384, at 315.

[495] Pelton, *supra* note 98, at 45.

[496] *Id.* at 76-77. For a comprehensive discussion regarding joint international regulation of airspace and outer space, *see generally Studies in Space Policy*, Vol. 7, *in* The Need for An Integrated Regulatory Regime for Aviation and Space: ICAO for Space? (Ram S. Jakhu et al., eds., 2011).

[497] Studies in Space Policy, *supra* note 496, at 42-43 & 53-64.

[498] *Id.* at 43; Pelton, *supra* note 98, at 76.

[499] Pelton, *supra* note 258, at 866; *see generally*, Studies in Space Policy, *supra* note 496.

[500] Frigoli, *supra* note 119, at 68.

[501] *Active Debris Removal, supra* note 20, at 38.

[502] Joseph S. Imburgia, *Space Debris and Its Threat to National Security: A Proposal for a Binding International Agreement to Clean Up the Junk*, 44 Vand. J. Transnat'l L. 589, 630 (2011); Pelton, *supra* note 258, at 857; Tian, *supra* note 319, at 123.

[503] Akers, *supra* note 384, at 311.

[504] Molly K. Macauley, *The Economics of Space Debris: Estimating the Costs and Benefits of Debris Mitigation*, 115 Acta Astronautica 160, 161 (2015).

[505] Akers, *supra* note 384, at 313.

[506] Macauley, *supra* note 504, at 163.

[507] Pelton, *supra* note 258, at 857.

[508] *Id.* at 859, 863.

[509] Tian, *supra* note 319, at 123.

[510] Emanuelli, et al,, s*upra* note 343, at 201; Macauley, *supra* note 504, at 163.

[511] Macauley, *supra* note 504, at 162; Pelton, *supra* note 258, at 858, 867; Tian, *supra* note 319, at 125.

[512] Imburgia, *supra* note 502, at 629.

[513] *Id.*; Timothy G. Nelson, *Regulating the Void: In-Orbit Collisions and Space Debris*, 40 J. Space L. 105, 113 (2015).

[514] Akers, *supra* note 384, at 313.

[515] Tian, *supra* note 319, at 123.

[516] Popova & Schaus, *supra* note 50, at 13.

[517] *See, e.g.*, UNFCCC, *supra* note 464, arts. 3(1) & 4(1).

[518] Mirmina, *supra* note 175, at 652-653; Pelton, *supra* note 98, at 77.

[519] *Active Debris Removal, supra* note 20, at 45; Mirmina, *supra* note 175, at 652-653.

[520] Akers, *supra* note 384, at 313-314.

[521] Jeff Foust, *Is it Time to Update the Outer Space Treaty?*, Space Rev. (June 5, 2017), http://www.thespacereview.com/article/3256/1.

[522] Popova & Schaus, *supra* note 50, at 12.

[523] *Active Debris Removal, supra* note 20, at 40.

[524] Viikari, *supra* note 154, at 759.

[525] *Active Debris Removal, supra* note 20, at 40.

[526] *See, e.g.,* National Space Legislation: A Comparative and Evaluative Analysis 162-165 (Annette Froehlich & Vincent Seffinga eds., 2018).

[527] *Active Debris Removal, supra* note 20, at 33.

[528] *Id.* at 34.

[529] Jakhu et al., *supra* note 9, at 131.

[530] Viikari, *supra* note 154, at 759.

[531] Popova & Schaus, *supra* note 50, at 12.

[532] U.S. Dep't of Def., Directive 3100.10, Space Policy ¶ 4(d) (Oct. 18, 2012, Inc. Change 1, Nov. 4, 2016).

[533] Pelton, *supra* note 258, at 857 & 860.

Ominous Oversight: The Usurpation of an Executive Agency's Right to Candid and Independent Legal Advice During Prohibited Personnel Practices and Retaliation Investigations and Prosecutions

*Major Ashley D. Norman**

* Major Ashley D. Norman, USAF, (LL.M., Labor and Employment Law, The George Washington University School of Law, with Highest Honors (2020); J.D., The Antonin Scalia School of Law, George Mason University (2012); B.S., Marketing and Economics, The University of Nebraska-Lincoln, with High Distinction (2009), is the Deputy Chief for the Labor Relations Branch at the Labor Law Field Support Center at Joint Base Andrews, Maryland. Major Norman is a member of the Nebraska bar. The author thanks Mr. Laurence Soybel and Professor Todd Peterson for their assistance with this article.

I. Introduction to the Dilemma Posed by the OSC Reauthorization Act of 2017

Imagine that you are a government attorney working in labor and employment law at the Environmental Protection Agency (EPA). You have been at this job for five years and through hard work and determination, you have built a lot of trust in the government officials you advise. They come to you for counsel on various issues. You have been working with a particular high-level official on a labor issue for the last two years to remove an employee for failure to perform his duties. In the midst of the process, this employee filed an Inspector General (IG) complaint against the high-level official that was unsubstantiated after a six-month investigation. After the IG complaint results were finalized, you are contacted by the Office of Special Counsel (OSC) and they demand all of your communications with this high-level official over the matter. As you start pouring through the hundreds of e-mails regarding this issue, you find e-mails discussing the legal merit of various actions but you also find e-mails where the official is venting to you about their frustrations about the labor and employment policies of the federal government and e-mails where he is venting about this particular employee. You know that turning over these e-mails not only harms the agency's legal position in what will likely be a finding of a prohibited personnel practice for retaliation, with a potential prosecution, brought to bear by the OSC,[1] but it also destroys the trust you have built over the last five years with this high-level official.

This precarious situation is now a reality for government attorneys that work for an agency that may find themselves the subject of an OSC investigation. The OSC is a small, yet powerful, independent agency that investigates whistleblower retaliation and prohibited personnel practices.[2] Despite the OSC's ability to access a large volume of non-privileged information,[3] the OSC became frustrated that executive agencies under investigation were withholding documents from the OSC based on the attorney-client privilege.[4] After providing testimony to Congress about this frustration in March 2017,[5] Congress explicitly provided in the Office of Special Counsel Reauthorization Act of 2017 that an agency's claim of common law privilege would not prevent the OSC from obtaining the privileged material.[6]

Other than OSC's word, there is no independent statutory guarantee that this privileged information will be protected from Congress or even the public. The OSC maintains that it takes steps to protect the privileged material and would not distribute the privileged material without agency consultation,[7] which is not defined. Agency consultation may be as minimal as notifying the agency of the intent to distribute. Without any definite guarantees preventing further distribution, OSC's access to privileged material will have a chilling effect on the free flow of

information between agency officials and agency attorneys. Even if there were statutory or regulatory restrictions on further distribution, the OSC is conducting an adversarial investigation into the agency and can bring claims for prosecution, and this alone will cause agency officials to be fearful that his or her discussions with agency counsel will be exposed.

It would be untenable to imagine that Congress could pass a law directing criminal defense attorneys to hand over all of his or her notes to investigators. While not directly analogous, the principles underlying the justifications for maintaining attorney-client privilege are not inapplicable to agencies, especially when the investigating agency can bring a case for prosecution. The touchstone for the application of the attorney-client privilege is the adversarial process.[8] The system is broken when we are required to hand over to prosecutorial bodies a blank check to obtain anything they want to obtain in aid of a prosecution. When government officials find out that discussions with their lawyers will be disclosed to an adversarial independent agency, they will avoid those discussions and the agency will be deprived of important legal advice.

Agency officials must be encouraged, when not acting adversely to the interests of the agency, to be open, honest and candid with the attorneys for the agency. A government attorney does more than simply recite the law—they provide confidential advice to agency officials that act within the scope of their employment. This confidential advice is protected by privileges rooted in the Constitution. It is of paramount importance to safeguard this confidential advice from disclosure to third parties so executive agencies can have the benefit of the sensitive discussions with their attorneys surrounding labor and employment decisions without fear of having their deliberations exposed. In line with the theory underlying attorney-client privilege,[9] the protection of these deliberations will result in the most effective legal representation.

In a question and answer sheet released by the OSC on its ability to access privileged material, the OSC compares itself to the Office of the Inspector General (OIG) in defense of its power to gain access to privileged information.[10] It is curious that the OSC chooses the OIG as a comparator. While Congress created the OIG under the guise of more accountability in government, one cannot ignore one of the other clear motives of Congress in establishing the OIG: access to more information.[11] By creating a plethora of reporting requirements, Congress was able to expand its access to executive information through strategically created IG positions.[12]

Despite the OSC's insistence that privileged materials provided to it will not be distributed to Congress without "agency consultation," a review of the *Fast and the Furious* ruling[13] demonstrates that an executive agency's concern about further disclosure is well founded. In that case, executive agency coordination with the OIG, which led to a public OIG report[14] on the matter, ended up weakening the agency's claim of privilege. The court found that even though the documents were protected under the deliberative process privilege, the disclosures in the public OIG report led to the agency being unable to articulate any harm that "it did not already bring about itself" and the court denied the claim of privilege.[15] Additionally, federal cases that recognize a governmental attorney-client privilege make it abundantly clear that to successfully claim the privilege, the agency must establish confidentiality at the time of the communication and then ensure confidentiality is maintained.[16]

For these reasons, this article recommends executive agencies stop providing privileged material to the OSC, at the direction of the Chief Executive. The law that requires the release of privileged information between executive branch agencies violates the constitutional doctrine of separation of powers. The requirement to turn over privileged material to the OSC unconstitutionally encroaches on the executive branch and weakens any future claims of privilege that executive agencies may wish to preserve. The President has a duty to resist unconstitutional provisions that encroach on powers of the presidency[17] and must protect the constitutionally recognized privileges that attach to the executive branch, which the President controls.

This article further recommends that until this dispute is decided by a court of law, the spirit of negotiation between, and within, the branches of government be resurrected[18] and executive agencies enter into negotiations with the OSC and Congress with the ultimate goal of implementing a system of independent review of the material the agency claims is privileged based on mutually agreed upon standards. An independent review will help allay the fears of the OSC that the privilege is being used to shield executive wrongdoing; while also reassuring the executive agency being investigated and prosecuted that material actually falling under a privilege will be protected.

In reaching these conclusions, this article will first provide an overview of the history, structure and statutory charge of the OSC. Next, it will analyze the relevant common law governmental privileges at issue. While some critics note that the rationale behind privileges are greatly diminished in the government context, courts have uniformly recognized the existence of executive privilege, the attorney-client privilege, and the attorney work-product doctrine in the governmental context.[19]

To conclude the background section, this article will address separation of powers concerns. Specifically, it will discuss whether Congress can constitutionally enact legislation governing the ground rules of information sharing of privileged material between two agencies in the executive branch and if it can, whether the executive has any basis in law to defy it. This article then addresses the related question of whether such a dispute is justiciable. Lastly, this article discusses the ultimate recommendation that the Chief Executive direct executive agencies to stop providing privileged material to the OSC and work with the OSC and Congress to establish an independent privilege review commission.

II. Background

A. History, Structure, and Statutory Charge of the OSC

The OSC was formed in an era defined by distrust in government. After the Watergate scandal erupted in 1972, Archibald Cox was appointed by the Attorney General to serve as the special prosecutor in the Watergate investigation.[20] Cox discovered that there were tapes recorded between President Nixon and his advisors that would very likely contain evidence of the crimes he was investigating and Cox subpoenaed them.[21] Even after being ordered to turn over the tapes by two courts, President Nixon refused to comply with the subpoena.[22] He offered a compromise by which a Senator from Mississippi, Senator John Stennis, would listen to the tapes and create summaries of the tapes that President Nixon could control.[23] When Cox rejected this compromise, President Nixon demanded the Attorney General and Deputy Attorney General fire Archibald Cox.[24] Both men refused and resigned.[25] Ultimately, the Solicitor General carried out the President's order and fired Cox.[26] This series of events is referred to as the Saturday Night Massacre.[27]

The Saturday Night Massacre highlighted several issues: (1) embedding the special prosecutor within the executive branch is problematic; and (2) special counsel are not immune to political whims.[28] While the OSC is separate and distinct from special prosecutors who investigate criminal allegations against executive officials, the OSC was created because of the problems of executive accountability that arose after the same officials they were directed to investigate fired "independent" prosecutors. After the Saturday Night Massacre, public confidence in the integrity of government was extremely low.[29] Congress needed to rebuild trust and reassure the American public that executive officials engaged in wrongdoing would not be immune from a fair and impartial investigation and would not be exempt from the consequences that may follow the substantiation of wrongdoing.[30]

Congress's primary effort to rebuild this public trust is manifested in the Ethics in Government Act of 1978, which created the U.S. Office of Independent Counsel, providing for independent counsel to investigate and prosecute criminal wrongdoing by high-level officials.[31] In the same vein, Congress also enacted the Civil Service Reform Act of 1978,[32] which established the Office of Special Counsel to investigate and adjudicate claims of prohibited personnel practices or other merit system protection violations in the federal government.[33] The Civil Service Reform Act of 1978 also established the Merit Systems Protection Board (MSPB). The MSPB is the board that hears employee appeals of agency actions that are brought before it.[34] As an independent agency, the OSC can bring cases to the MSPB for prosecution and can prosecute cases in front of the board.[35] Initially, the OSC and the MSPB were part of the same organization but they were separated into two distinct independent agencies in 1984.[36]

The head of the OSC, known as the Special Counsel, is appointed by the President with the advice and consent of the Senate.[37] The Special Counsel may be removed by the President only for inefficiency, neglect of duty, or malfeasance in office,[38] which serves as indicia of the independence of the agency.[39] Interestingly, when the bill was presented to President Reagan providing for the separation of the MSPB and OSC, he vetoed the bill.[40] President Reagan objected to an independent OSC because he believed it would unconstitutionally limit his powers of supervision and removal.[41] However, unlike *Bowsher* and *Myers,*[42] Congress did not try to retain a role in the removal process for OSC officials. Thus, the OSC arrangement is arguably more akin to *Morrison* where the Supreme Court found that the limitations on removal placed on the President for the independent counsel assigned to investigate criminal wrongdoing did not interfere with the constitutionally assigned functions of the executive branch or violate the constitutional doctrine of separation of powers.[43] The removal provision here still gives the President ample authority to remove a Special Counsel.[44]

However, the Court in *Morrison* seemingly glosses over the fact that Congress receives reports and other information from the independent counsel and can still conduct oversight.[45] The Court simply states that these are functions that have been recognized as being "incidental to the legislative function of Congress."[46] What the Court fails to recognize is this function is precisely where many of the separation of powers issues originate. To what extent Congress can expand reporting requirements and oversight to obtain information, especially privileged information, about the inner workings of the executive branch remains an open question that is largely resolved by compromise or by courts on a case-by-case basis. As is argued in this article, access to executive branch information that is privileged is not "incidental to the legislative function of Congress" and presents

grave separation of powers concerns. It is of little consequence that the information seizing is under the guise of the OSC, which is technically in the executive branch, because Congress not only creates the OSC, but the OSC is dependent on Congress for its continued funding.

The OSC lists several scenarios on its website where it may disclose information, potentially of a sensitive or personal nature, to third parties.[47] One of the scenarios is that the OSC may turn over files to a congressional committee or subcommittee having jurisdiction over the matter in the files.[48] Additionally, the "Special Counsel … *shall* transmit to the Congress on the request of *any* committee or subcommittee thereof, by report, testimony, or otherwise, information and the Special Counsel's views on functions, responsibilities, or other matters relating to the Office."[49] If you visit OSC's website, you can see public records of testimony given to Congress where this command to testify about "functions, responsibilities, or other matters" turned into testimony on various investigations conducted by OSC.[50]

This highlights why the new law permitting the OSC to refuse to recognize an agency claim of a common law privilege is controversial—the information is not confined by statute or regulation for OSC's use. In fact, in her Congressional testimony to advocate for the provision to refuse to recognize agency claims of privilege, former Special Counsel Carolyn Lerner claimed it is "impossible" to determine if there has been retaliation without knowing the motivation of the personnel actions, which would be revealed in the privileged material. She also testified to Congress that using a privilege to shield information from OSC is inconsistent with OSC's statutory mandate to investigate prohibited personnel practices.[51] These statements indicate that former Special Counsel Lerner believes executive agencies are concealing wrongdoing under the guise of a claim of privilege. Yet she points to not one example where this was the case.

Shortly after Special Counsel Lerner provided this testimony, Senator Ron Johnson, a Republican Senator from Wisconsin, introduced the bill in the Senate.[52] The Committee Report on the bill is relatively silent on the discussion of the attorney-client privilege. The report quotes Special Counsel Lerner's position on the matter, but there is a dearth of substantive discussion on the implications of this provision on executive decision-making.[53]

B. Governmental Privileges and Executive Agencies

To best understand the application of this new provision permitting OSC to decline to recognize claims of common law privileges, it is helpful to review the

most relevant common law governmental privileges. While there are many privileges recognized at common law, this article focuses on the privileges that are most applicable to executive branch officials when they are receiving advice from agency attorneys: the attorney-client privilege, the work product privilege, and executive privilege.

1. Attorney-Client Privilege

In her testimony to Congress, former Special Counsel Lerner makes a point to note that "no court has ever held that the attorney-client privilege can be asserted during intra-governmental administrative investigations."[54] She then quotes *Upjohn Co. v. United States*, 449 U.S. 383, 389 (1981) to explain the purpose of the attorney-client privilege: to encourage "full and frank communication between attorneys and their clients and thereby promote broader public interests in the observance of law and the administration of justice."[55] She states that asserting the privilege in the context of an OSC investigation is inconsistent with this purpose for three reasons: (1) there is a strong interest in exposing government wrongdoing; (2) review by the OSC does not deter full and frank discussions because agencies repeatedly provide this sort of information to OSC to prove they acted lawfully; and (3) there is no precedent to support that disclosure would constitute a waiver of the privilege in another context.[56] This article addresses each in turn.

To begin, *Upjohn* is a peculiar case for Special Counsel Lerner to cite to because in that case, the Supreme Court upheld an application of the attorney-client privilege to corporations, thereby accepting a more expansive application of the attorney-client privilege.[57] Additionally, she fails to even acknowledge that courts have considered, and routinely endorsed, the application of a governmental attorney-client privilege in the civil context, particularly when considering the application of exemptions under the Freedom of Information Act (FOIA).[58] The FOIA was enacted to establish a statutory right of public access to executive branch information in the federal government.[59] Its purpose was to create an informed citizenry that can serve as a check against corruption in government.[60] Although the FOIA broadly favors disclosure,[61] there are nine categories that are exempt from disclosure that, in the estimation of Congress, serve to reach a workable balance between an informed citizenry and the government's need to protect certain information.[62] The most relevant exemption to this article is exemption five, which exempts from disclosure intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency.[63]

Courts considering exemption five have recognized that despite a strong interest in exposing government wrongdoing, the governmental attorney-client privilege is a vital aspect to effective functioning of government. In the *Coastal Gas* case, the Court of Appeals for the District of Columbia notes that courts have recognized documents that would be protected under the attorney-client privilege, the work product privilege, and the executive "deliberative process" privilege as being protected under exemption 5 of FOIA.[64] The court notes that it is "clear" that an agency can be a client and agency lawyers can be attorneys within the relationship contemplated by the privilege.[65] However, the court ultimately found that the agency attorney's neutral interpretations of objective regulations were not covered by privilege.[66] Of note to the court, the agency failed to establish confidentiality, both at the time of the communication and failed to maintain confidentiality since.[67] The agency admitted it had no idea who had access to the documents.[68] Accordingly, the protections of attorney-client privilege, and thus the protections of exemption five, did not apply to the agency attorney's neutral interpretations of regulations that were not established to be based on confidential communications.[69]

The same court also considered governmental attorney-client privilege in the *Mead Data* Case.[70] There were several documents in *Mead Data* that were sought under exemption five of FOIA and consisted of legal opinions and advice.[71] The court found that exemption five did indeed encompass a governmental attorney-client privilege.[72] The court considered the policy objective of exemption five.[73] The court noted that exemption five is intended to protect the free flow of information to agency decision makers and this "certainly" includes advice on legal questions.[74] However, similar to the court in *Coastal Gas*, the court found that there was no indication that the documents at issue were based on confidential information provided by the client.[75] Accordingly, the court declined to apply the protection.[76]

Notably, *Mead Data* and *Coastal Gas* deal with disclosure of certain materials to the public, rather than intra-governmental disclosures. However, in both decisions, the courts acknowledge the existence of agency privilege, and specifically assert that governmental agencies can have an attorney-client privilege with agency attorneys.[77] Both courts place a value on the free flow of advice to agency decision-makers, thus showing a willingness to place limits on transparency for the sake of effective government. The court in *Mead Data* even quotes one of the congressional reports on FOIA that if government were forced to operate in a fishbowl, then the "full and frank exchange of ideas on legal or policy matters would be impossible."[78]

Despite former Special Counsel Lerner's failure to acknowledge these important considerations for executive agency decision making, she also fails to account for the fact that government attorneys have ethical duties that prevent them from concealing wrongdoing.[79] Therefore, even in the absence of the OSC Reauthorization Act of 2017, there are institutional barriers that prevent government attorneys from condoning or concealing criminal wrongdoing by government officials.[80] The OSC Reauthorization Act of 2017 paternalistically assumes that government attorneys are not handling those ethical obligations in accordance with his or her professional obligations.

Yet ethical obligations may vary depending on whom a government attorney considers as the "client." Most government attorneys would agree that individuals within the entity do not hold the privilege personally.[81] By way of example, within the Department of the Air Force, Judge Advocate Generals (JAGs) regularly advise individual military commanders, yet a JAG's "true client" is the United States Air Force.[82] Government lawyers assist agencies in determining the requirements of legislation, assessing the legality of proposed actions, and evaluating possible avenues of enforcement,[83] all for the benefit of the *agency*.[84] Government lawyers have no obligation to the desires of any one individual, especially if those desires do not benefit the agency.

Although the Air Force has, by policy, stated that confidences disclosed to JAGs by Commanders "must be treated as privileged to the greatest extent allowed by law,"[85] the law would require disclosure in many situations because the attorney's ethical obligations are to the agency. For instance, if a Commander tells a JAG that he knows it is wrong to keep his government computer to use it as his personal computer after he moves to a new assignment, but he is going to do it anyway, the JAG would have to disclose the misappropriation.[86] That is an obvious situation where the communication by the commander is adverse to the interests of the agency and the attorney's ethical obligations are to the agency—not the individual Commander. However, stating the obvious serves the important purpose of demonstrating that a governmental attorney-client privilege is not necessarily incompatible with the exposure of wrongdoing in government.

Admittedly, where things get more complicated is when the wrongdoing may not be so obvious. Alternatively, perhaps, there may not be any significant wrongdoing at all. For example, there may be a few off-handed comments that are not illegal per se; but rather they cause the agency to be viewed in a negative light. To illustrate, lets return to the hypothetical of the high-level EPA official removing an employee for poor performance. This employee has also made numerous complaints against the official for discrimination and favoritism which were unsubstantiated after

an internal investigation. Imagine the high-level official tells you that he has lost confidence in the employee after the employee tried to report him for wrongdoing and wants to base the removal action on poor performance and loss of confidence. You will likely advise the official that by including "loss of confidence" based on protected complaints, that he or she may be subject to a retaliation claim, and it will be cleaner and easier to just base the action on the overwhelming evidence of poor performance.

If the OSC steps in and requires you to disclose this advice and the official's comments, the OSC will probably pursue a retaliation claim. Despite the fact that the employee was, in fact, a substandard performer and in spite of the fact that all of the complaints by this employee were unsubstantiated, the OSC may seek disciplinary action against the supervisor once they receive this information. Resources will be poured into a prosecution that puts the agency between a rock and a hard place: they either win the case and waste more time and energy dismissing a poor performer, or they lose in spite of the overwhelming evidence of poor performance and have to retain him. Either way, this situation does not further the public interest and only deters the frank discussions that courts deem essential between officials and their attorneys. In a world where this is at stake, there is no way the official would ask for your thoughts on adding a loss of confidence claim knowing that everything he approaches you with will be disclosed and used against him or her.

With regard to the OSC, the traditional justifications for the attorney-client privilege[87] that former Special Counsel Lerner dismisses are even stronger because the OSC itself can bring a case forward for prosecution. Though the OSC is technically lodged in the executive branch, it has a rulemaking function and a prosecutorial function. The OSC can bring cases to the MSPB that can result in disciplinary action.[88] In fact, pursuant to the OSC Reauthorization Act of 2017, if the OSC substantiates a claim, the proposal of discipline is mandatory.[89] This is undoubtedly an adversarial process from the standpoint of the agency and contrary to former Special Counsel Lerner's assertions that the privilege is unnecessary, this is actually where the justifications for privilege is at its apex.

Further, along in her testimony, former Special Counsel Lerner explains it would be "impossible" to determine if there has been retaliation without knowing the motivation underlying the personnel actions at issue, which would be disclosed in the privileged communications.[90] This assertion is simply untrue. The OSC can still investigate the actions taken, interview witnesses, and have access to any nonprivileged document surrounding the action in the course of their investigation. You can certainly uncover motivations and draw reasonable inferences about

motivations without accessing privileged material, and wrongdoing can still be exposed. Consider the plethora of substantiated OSC investigations within the last decade.[91] In spite of the assertion of certain privileges, the OSC has still been able to perform its functions. This contradicts her assertion that privileges make the exposure of wrongdoing "impossible."

By way of example, imagine again the hypothetical of a requirement for a defense attorney to turn over all of his notes with his client to the police. Imagine the police department's justification was that it is "impossible" to know if the requisite intent existed without these notes. This would certainly not justify such an invasive requirement that runs counter to our entire system of justice. There are distinctions to be made between that example and the OSC Reauthorization Act of 2017. However, the example illustrates that although there are factors that would make an investigation easier (such as access to privileged material), there are certain constructs, including the attorney-client privilege, that we have deemed as a society to be important enough that we are willing to place some limitations on transparency for the preservation of our adversarial system.

It should be difficult for an adversarial agency to punish an agency or agency officials. There should be standards and burdens, and there should be information the agency can receive from its own attorneys without worrying about the information being used as the basis for adverse action. In addition, to end this discussion where we started, the courts have recognized that this privilege "certainly" exists in the governmental context.[92]

Former Special Counsel Lerner also asserts the OSC is entitled to privileged information because agencies give much of this information to the OSC anyway to prove the agency acted lawfully.[93] This again goes to the heart of the OSC's assessment of the motivations of government attorneys: that they conceal incriminating evidence. This assumes government attorneys do not take their professional obligations seriously. However, Special Counsel Lerner provides no evidence of this supposed concealment. In fact, she fails to cite even one case of a government attorney engaged in such misconduct. Additionally, she also seems to argue that an affirmative limited waiver of a privilege should be considered a full waiver of privilege, in the face of the caselaw that states otherwise.[94]

Lastly, former Special Counsel Lerner notes that there is no precedent to support that disclosure would constitute a waiver of the privilege in another context.[95] The *Fast and the Furious* decision, decided the year prior to her testimony, indicates otherwise. In that case, agency cooperation with the OIG and a subsequent publication of the OIG report weakened the agency's claim of privilege so much so that

the judge rejected the claim of privilege.[96] Just browsing through the hundreds of pages of Congressional testimony and public reports on the OSC's website,[97] it will become clear that an executive agency's concern of disclosure is a valid one. There are no statutory or legal restrictions preventing the OSC from further disclosing information provided to it. The OSC's close relationship with Congress and general practice of publishing a vast amount of information on its website lends support to this article's recommendation that executive agencies cease providing privileged material to the OSC.

2. Attorney Work Product Privilege

Many courts have held that communications by, or for, government attorneys are covered under the work product doctrine.[98] Under the work product doctrine, an opposing party cannot discover the work product, including ideas and litigation strategy, of another attorney.[99] The work product privilege doctrine is judicially created and found its inception in *Hickman v Taylor*.[100] In *Hickman*, the Court based its decision on the proper preparation of a case.[101] If the attorney's work were turned over to opposing counsel, the court noted that "much of what is now put into writing would remain unwritten."[102]

Though it has been found that the attorney work-product privilege applies to the government under exemption five of FOIA, there is a very important limitation to the application of the privilege: it only applies to documents prepared in anticipation of litigation.[103] Generally, this means it is initially prepared in contemplation of litigation or in the course of preparing for trial.[104] Under exemption five of the FOIA,[105] which exempts from disclosure inter-agency or intra-agency memorandums or letters which would not be available by law to a party in litigation with the agency, attorney work product is exempt from mandatory disclosure without regard to the status of the litigation for which it was prepared, as long as the litigation was contemplated when the document was created.[106]

The Supreme Court has noted that it was "clear" Congress had the attorney work product privilege in mind when it adopted FOIA exemption five.[107] The Supreme Court explained that the Senate report on FOIA states exemption five "would include the working papers of the agency attorney and documents which would come within the attorney-client privilege if applied to private parties."[108] The Supreme Court also pointed out that the case law has extended the attorney work-product rule of *Hickman* to government attorneys in litigation.[109] The Supreme Court found that memoranda, which directed the filing of a complaint, fell "squarely" within exemption five's protection of attorney-work product because

the memoranda were prepared in contemplation of litigation and did not reflect final decisions of the agency.[110]

The Fifth Circuit even found that agency investigatory reports that were prepared very early in the case were protected under the work product doctrine.[111] The court considered the fact that an Unfair Labor Practice (ULP) charge had already been filed in finding that a specific claim had arisen, and thus the prospect of litigation was identifiable.[112] In contrast, however, the court in *Coastal Gas* made clear that the discussion of "specific factual situations" that may have happened to turn into litigation matters is not sufficient for the privilege to apply.[113] Therefore, in the context of OSC investigations of agency labor practices, the application of the work produce doctrine will likely turn on when and in what manner the agency was notified of the formal charge.

Application of the work product doctrine may also turn on whether litigation was a "substantial likelihood" or a "remote possibility,"[114] but the subsequent outcome of whether or not litigation ensues is not dispositive.[115] Given that the OSC can bring disciplinary and corrective action cases to the MSPB for prosecution, a notification of an OSC investigation may be sufficient for an agency to claim work-product privilege for documents prepared after this notification. However, if the agency were to receive general legal advice on its actions before the OSC were investigating, this would make the work-product privilege more difficult to successfully claim, particularly if the employee had never made a complaint or filed a grievance before. There would then likely be a case-by-case determination as to the agency's thoughts on the likelihood of litigation at the outset of the claim, and this can differ markedly based on the complainant.

Of note, for the work product doctrine to apply, the agency has the burden to show that a specific claim had arisen, it was disputed by the agency, and it was discussed in the memorandum.[116] Thus, with regard to OSC investigations, the agency may have to show that a prohibited personnel practice or whistleblower retaliation claim was alleged, the agency disputed the claim, and that the memoranda were regarding the disputed allegation. Similar to a claim of attorney-client privilege, the agency will also likely have to show there were attempts to maintain the confidentiality of the disputed documents. The importance of maintaining confidentiality for future claims of privilege again lends support to the recommendation that executive agencies, with the consent of the Chief Executive, stop turning over these documents, which is discussed further in Part III.

3. Executive Privilege

Executive privilege is the constitutional prerogative of the President to withhold certain information from Congress.[117] The practice dates back to President George Washington, who refused to produce all of the documents sought by the House of Representatives related to negotiations of the Jay Treaty of 1795.[118] This began a long-standing tradition of the President invoking executive privilege to protect the executive decision-making process; the existence of which has not since been doubted by Congress.[119] Past Presidents have claimed it on everything from advice on presidential appointments[120] to memoranda regarding prosecutorial decisions,[121] primarily based on the rationale that the existence of the privilege allows the chief executive to receive candid advice.[122] While the protections are strongest for Presidential communications, there is also a deliberative process privilege that "reaches beyond conversations with the President to protect other communications among executive branch officials 'crucial to fulfillment of the unique role and responsibilities of the executive branch.'"[123]

Typically, disputes over executive privilege have been resolved by negotiation and accommodation.[124] The branches have traditionally not turned to the courts for the solution. However, there may be more of a trend to seek the involvement of the courts due to the widespread use of executive privilege in the Trump Administration. In fact, a Department of Justice attorney admitted that there has never been such a broad-scale defiance of requests for congressional information in the history of the republic than with the Trump Administration's repeated refusals to provide information in response to congressional requests for information.[125] President Trump and his attorneys made broad claims of executive privilege that they maintained were applicable even in impeachment proceedings.[126] These broad assertions have highlighted Congress's limited tools in the face of an executive willing to broadly assert executive privilege.

Turning to the judicial system for a resolution of a dispute over executive privilege is not the optimal solution for either branch. First, the judicial process is by no means an expedient way to resolve the dispute. This can be particularly challenging for Congress, because a congressional subpoena is only valid until the expiration of the term.[127] Second, there is no guarantee that a court will resolve the merits of an executive privilege dispute between the branches. While several federal courts since *Nixon* have done so, a recent decision out of the D.C. Circuit Court of Appeals declined to decide the case on the merits and found that the dispute did not present a case or controversy under Article III (which will be discussed further in Section II(C)).[128] Further complicating the matter is that the OSC (an independent executive agency) and traditional executive agencies,

such as the Department of the Air Force, both fall under the executive branch. Thus, the cases where the court did reach the merits on a claim of privilege by the executive in the face of a congressional subpoena may not even be applicable here. While the separation of powers discussion will delve into several of these cases and issues, suffice it to say that the jury is out on whether a court would find the privilege dispute between the OSC and executive agencies to be justiciable. Lastly, presenting the court with an executive privilege dispute is inherently risky for both branches. An unfavorable ruling would substantially reduce the power of either branch.

For example, the executive branch lost the battle in *United States v. Nixon*[129] but won the war. Although the court ultimately found that the President's generalized interests in confidentiality cannot prevail over the fundamental demands of due process of law in the fair administration of criminal justice, the Supreme Court recognized that executive privilege is "inextricably rooted in the Constitution."[130] The court recognized for the first time a presumptive privilege in favor of Presidential communications.[131] Although this is favorable for the executive, it also set the stage for the courts to be the arbiter of how far the privilege will extend. This creates separation of powers issues for all three branches, which will be discussed further in Section II(C).

Before moving on to that discussion, it is worthwhile to discuss executive privilege claims not involving Presidential communications, as that is the situation most analogous to the privilege claims by executive agencies in the course of OSC investigations. While the President himself does not direct the claim, the claim by other executive officials helps the President fulfill his constitutional duties. The Supreme Court has had the occasion to consider agency deliberations not involving an explicit Presidential communication in *NLRB v Sears Roebuck & Co.*[132] The Supreme Court found that Congress had executive privilege in mind when it adopted exemption five of the FOIA.[133] The Supreme Court shared the concerns of Congress and agreed with other courts that agency decision-making would be negatively impacted if discussions on legal and policy matters were made public.[134] However, the court notes that only predecisional communications are privileged.[135] The Supreme Court said exemption five could never apply to final agency decisions.[136]

Lastly, it is worth returning to the *Mead Data* case because that case also speaks to the context of agency deliberations not involving an explicit presidential communication, which is what is at stake under the OSC Reauthorization Act of 2017. In *Mead Data*, the court found that exemption five did apply to "discussions among agency personnel about the relative merits of various positions which might

be adopted in contract negotiations" with a private party.[137] The court noted that not only does the recommendation deserve protection, but so do the discussions or advice that went in to the formulation of the recommendation.[138] The court even expressed that in some circumstances, purely factual information will be protected under this privilege.[139] The court relied on the fact that the "deliberative process" deserves protection under exemption five because the quality of administrative decision-making would be seriously undermined if agencies were "forced to operate in a fishbowl."[140] Interestingly, it appears that the discussions at issue did not even involve attorneys; rather they were between agency officials. The application of these principles would only be strengthened when the advice and discussions involve agency counsel.

To recap, many of the most impassioned disputes between the executive and legislature develop because of the executive branch's claim of executive privilege.[141] Congress does not have many options at its disposal when it disagrees with a claim of executive privilege—Congress can attempt to establish standing and obtain judicial review[142] and wait years, or pursue impeachment,[143] which can also be a lengthy process and takes a supermajority to convict. Impeachment is also made more difficult in the face of executive defiance. Based on this, the discussion of executive privilege blends well into the next section of separation of powers.

C. Separation of Powers

The Constitution sought to divide the delegated powers of the federal government into three defined categories, legislative, executive, and judicial, to ensure that each branch would confine itself to its responsibilities.[144] As government has grown and delegation is commonplace, it gets increasingly more difficult to identify to which branch a power belongs.[145] This has led the Supreme Court to endorse a more functional approach to the separation of powers, where courts will generally uphold comingled functions where there is no concern over aggrandizement or encroachment.[146] If one branch accumulates too much power or undermines the authority or independence of another branch, then the constitutional doctrine of separation of powers is violated.[147]

The provision in the OSC Reauthorization Act of 2017 giving OSC access to privileged information goes to the heart of many separation of powers issues: to what extent can Congress pass laws that restrict implied constitutional powers of the executive? One of the foremost cases on Congress's authority to control executive materials is *Nixon v. Administrator of General Services*.[148] The case involved the constitutionality of the Presidential Recordings and Materials Preservation Act.[149] In upholding the Act, the Supreme Court found that for separation

of powers, the proper inquiry focuses on the extent to which the Act prevents the Executive Branch from accomplishing its constitutionally assigned functions.[150] Only where the potential for disruption is present must the court then determine whether that impact is justified by an overriding need to promote objectives within the constitutional authority of Congress.[151] The court found Congress's need to preserve the materials and maintain access to them for lawful governmental and historical purposes outweighed the claims of presidential privilege.[152] Notably, the archivist screening the privileged material did not have any independent ability to bring a prosecution and the screening was accommodative—not adversarial. This difference is extremely important because the OSC does not give the agency any opportunity to justify the privilege; rather they wholescale refuse to recognize its existence.

Because the executive agency can be subject to prosecution by the OSC and the law unconstitutionally encroaches on constitutionally-based executive functions, the executive has a basis to withhold privileged information from the OSC.[153] While Congress is vested with the power to make laws, we know that this power is not absolute and/or unreviewable.[154] While judicial review is contemplated or pending, the executive can refuse to defend or enforce a law if it believes the law will be struck down.[155] This is part of the President's oath to support and defend the Constitution, and in former Attorney General Edwin Meese III's view, it is the duty of all three branches to play a role in assessing the constitutionality of government action.[156]

The ability to assess the constitutionality of a law is particularly important today, where the functional approach to the separation of powers does not involve the application of "bright line" rules. In modern government, it is extremely difficult to assess what branch the action belongs to in the first place.[157] In fact, the functional approach to separation of powers is arguably more akin to Justice Stewart's views on the obscenity doctrine: "you know it when you see it."[158] While reasonable minds may differ as to how to label the action, many of the cases reflect an underlying sense of optimism that when the powers are imbalanced, we can trust our government to perceive the imbalance, "know it when they see it," and address it. The harsh reality is that there are not many processes in place that actually provide for a successful resolution of comingled functions that result in aggrandizement or encroachment.

One big complicating factor is that, as mentioned above, it is difficult to mount court challenges for disputes between Congress and the executive.[159] Ordinarily to get judicial review, an executive official must accept a citation for contempt of congress and await court action to enforce it.[160] Even if a contempt citation is

issued, one of the reasons compromise outside of the courtroom is so important is because courts are frequently hesitant to intervene in inter-branch disputes and often, the branches do not want judicial intervention either.[161]

Under the political question doctrine, the court may decline to decide issues that are "committed" to one of the branches.[162] One of the leading cases on the doctrine is *Baker v Carr*, where the Supreme Court ruled there is a non-justiciable political question when there is a textually demonstrable constitutional commitment of the issue to one of the political branches or a lack of judicially discoverable and manageable standards for resolving the issue.[163] Executive privilege is a privilege "inextricably rooted in the separation of powers under the Constitution,"[164] but it is not necessarily a *textually* demonstrable commitment. Additionally, looking at the *Fast and Furious* and *Nixon* cases as examples, both courts decided that the scope and application of executive privilege was justiciable.[165] The district court in the *Fast and the Furious* case actually cited *United States v Nixon* in that the court not only had the authority, but the responsibility, to resolve the conflict.[166] These decisions show that under the standard articulated in *Baker v Carr*, there are likely discoverable and manageable standards that courts have applied to this issue despite there being no clear textual commitment.

The court in the *Fast and the Furious* case found that it had the authority to rule on the scope of executive privilege.[167] In that case, the Committee for Oversight and Reform issued a subpoena to the Attorney General for records relating to Operation Fast and Furious and the executive branch asserted executive privilege.[168] The Court found that "records reflecting the agency's internal deliberations over how to respond to Congressional and media inquiries falls under the protection of the deliberative process privilege."[169] However, the court then said that the Plaintiff's need for the documents outweighed the concerns that underlie the privilege in this case because the documents were already made public through an OIG report.[170] The court found that even though the IG report did not attach the documents in full, there was enough information provided in the report to greatly diminish any argument that further disclosure would result in any harm.[171] Thus, the agency's cooperation with the OIG negatively impacted their claim of privilege in the face of a congressional subpoena.[172]

Another case addressing the scope of executive privilege is *United States v. AT&T*.[173] In that case, the house oversight committee subpoenaed AT&T for documents concerning wireless wiretapping.[174] The Department of Justice sued to enjoin AT&T from disclosing the documents on the basis of national security.[175] The district court granted the injunction but the court of appeals remanded and suggested parties reach a settlement based on guidelines proposed

by the court.[176] The Court noted that the framers believed there would be compromise in the face of their generality in favor of effective government.[177] In the face of a conflict, "each branch should take cognizance of an implicit constitutional mandate to seek optimal accommodation through a realistic evaluation of the needs of the conflicting branches in the particular fact situation."[178] While the court in AT&T declined to get involved with the minute details of the settlement, the court did say that it will involve itself by accepting a structure that includes the availability of the court to resolve relatively narrow issues, through *in camera* inspection of the back-up memoranda to verify the accuracy of the generic description supplied by the Executive.[179] As to justiciability, the court noted the political question doctrine was only appropriate when a branch "has a clear and unequivocal constitutional title,"[180] which was not the case here.

The court recently decided to hear the case of *Committee on the Judiciary, U.S. House of Representatives v Miers*.[181] This case involved a clash between Congress and the Executive. In the *Miers* case, the Department of Justice requested and received resignations from seven US attorneys under suspicious circumstances.[182] The Committee on the Judiciary commenced an investigation and the executive provided many materials, but the Committee asserted they required the testimony of a former White House counsel, Ms. Miers, about her role in the decision to fire the attorneys.[183] Ms. Miers refused.[184] After a long period of negotiation, the parties reached a self-declared impasse with respect to the document production and testimony of Ms. Miers.[185] The full house voted to hold Ms. Miers in contempt of Congress and certified the contempt report to the United States Attorney for D.C. to pursue criminal enforcement of the contempt citations.[186] The Attorney General then directed the U.S. attorney not to prosecute Ms. Miers,[187] at which point the Committee filed its lawsuit.

The Court noted that after *Nixon*, courts are the final arbiter of executive privilege.[188] The court stated allowing the executive to determine the limits of its own privilege would "impermissibly transform the presumptive privilege to an absolute one."[189] The Court noted the executive could not cite to a single judicial opinion recognizing absolute immunity for senior presidential advisers,[190] but then went on to note that even if they could, Congress would be left with no recourse to obtain information that was not privileged.[191]

The Court then considered that there are timing concerns and potential mootness issues because Congress expires every two years and a subpoena remains valid for only the duration of that Congress.[192] The Court found that concern does not counsel against hearing the case.[193] Based on the caselaw just discussed, it is highly likely that if executive agencies were to stop providing privileged

documents to the OSC in defiance of the law, a court would find that the dispute would be justiciable. Modern courts have largely declined to find that executive privilege is a textual commitment to the executive branch, instead implying that its scope is a legal question to be decided by a court. However, as the *Miers* court correctly observes, there are often timing concerns. The next section proposes a similar review to be accomplished by a commission under mutually agreed upon standards, thus providing a faster mechanism for the branches to sort through these claims and for Congress to get that "second look" the court in the *AT&T* case mentioned.[194]

Though it may seem that in the wake of the decisions just discussed, judicial intervention in governmental information disputes can be fairly assumed, the United States Court of Appeals for the District of Columbia Circuit recently declined to decide the case involving a congressional subpoena of former White House Counsel Donald McGahn for documents related to obstruction of justice by President Trump.[195] McGahn, at the direction of the President, claimed absolute immunity and refused to comply with the subpoena.[196] The Court said it lacked authority to resolve disputes between the executive branch and the legislative branch until their actions harm an entity beyond the federal government.[197] The court found that McGahn's refusal to comply with a congressional subpoena had no bearing on the rights of individuals or some entity beyond the federal government.[198] Although the court conceded that the dispute was sufficiently adverse, the Court seemed to say that actually worked against judicial intervention because it would displace the historical preference for negotiation and accommodation.[199] The court brushed aside the argument that subpoena enforcement was the type of dispute typically resolved by the courts by noting that historically, lawsuits between the executive branch and legislative branch did not exist.[200] Lastly, while not based on a legal principle, the court provides a prudential concern in that the "the walk from the capitol to our courthouse is a short one, and if we resolve this case today, we can expect Congress's lawyers to make the trip often."[201]

While the *McGahn* decision is in stark contrast to the *AT&T*, *Miers*, and *Nixon* decisions in which the courts did reach the merits, the D.C. Circuit took the case *en banc*.[202] Thus, at the time this article was written, the status and precedent of the *McGahn* decision is uncertain. In the context of the privilege dispute caused by the enactment of the OSC Reauthorization Act of 2017, assessing whether or not a court would decide the case also involves consideration of the fact that this dispute is entirely within the executive branch at this point. Congress does not have as strong of an argument for standing as it did in *McGahn*, *AT&T*, *Miers* and *Nixon* because the case does not involve congressional subpoenas or requests for information pursuant to its oversight responsibilities. Rather, it involves congressional

delegation of oversight to an independent agency, which is more attenuated. The dispute does, however, involve compliance with a duly enacted statute, which may form some basis of an institutional injury claim. Courts have allowed Congress to defend statutes that the executive claims are unconstitutional.[203]

Whether or not the OSC itself would have standing to sue an executive agency is a question that is also largely unsettled. Many cases analyzing issues under the separation of powers doctrine look for an actual conflict of sufficient adversity to find the case justiciable, and some may believe that to be impossible in a unitary executive.[204] However, if one follows the rationale of *Humphreys Executor*, it may be argued that the interests of independent agencies can, and sometimes must, be adverse to executive interests.[205] This adversity may be adequate to provide the opportunity for judicial resolution, despite the agencies being in the same *branch*. Even the Court in *Myers*, which is an opinion that unitary executive theorists hold near and dear, concedes that in certain circumstances Congress can limit the discretion of an officer so much so that the President cannot direct the action of that officer,[206] thereby creating situations where adversity will exist in the executive. Given that the OSC can bring cases against executive agencies for prosecution, a court would probably find it to be sufficiently adverse as to be resolved by the judicial branch, despite the fact that it is an intra-branch conflict. In *United States v. Nixon*, one of the seminal cases on executive privilege, President Nixon argued the dispute was an intra-branch conflict.[207] The Court stated that the mere assertion of an intra-branch dispute has never served to defeat federal jurisdiction.[208]

One last factor worth mentioning is that the cases discussed above that address separation of powers concerns primarily involve battles between the executive branch and the legislative branch. The problem posed in this article is between an independent executive branch agency and another executive branch agency. If a court were to deem the OSC to be an arm of Congress rather than an arm of the executive, then the principles in the cases discussed may be more relevant. Until then, the OSC is technically an independent executive branch agency. Thus, this article's proposed solution may be simpler than the issues the courts above grapple with. As discussed next, if they are all lodged in the executive, then to put it simply: the President, as the Chief Executive, can do whatever he or she believes is constitutionally required, particularly if you subscribe to a unitary executive model.

III. Recommendations

A. At the Direction of the Chief Executive, Executive Agencies Must Withhold from Providing the OSC with Privileged Documents

With the blessing of the Chief Executive, the first step is for executive agencies to stop giving privileged material to the OSC. The provision requiring privileged material to be turned over to the OSC should not be followed for two primary reasons: (1) the OSC Reauthorization Act of 2017 violates the constitutional doctrine of separation of powers; and (2) to maintain the privilege in other settings, the agency must assert the privilege consistently and must not disclose privileged information to other agencies, including the OSC.

To be clear, not all of the conflict created by the presence of the OSC is unwanted by the Chief Executive. The President has a vested interest in ferreting out wrongdoing among his subordinates, and the OSC mission is a crucial part of the President's strong interest in an honest and efficient government. Where the OSC goes too far is requiring privileged information, including information subject to the attorney-client privilege and executive privilege, to be disclosed to them pursuant to their investigations. This is the provision that violates the doctrine of separation of powers.

By way of analogy, imagine the executive branch is a human body. The President is the brain, directing and guiding action. The OSC represents white blood cells, seeking out and destroying viruses within the system. However, if the white blood cells become too powerful and begin harming healthy tissue as well as destroying viruses, the brain's idea should not be to shed itself entirely of white blood cells. Instead, it should find a way to bring those white blood cells back into balance, where they only take out the viruses and leave the healthy tissue intact. The President, as the Chief Executive, has a duty to maintain the equilibrium. In this case, that means protecting privileged documents. Without access to privileged documents, the OSC still fits in to the unitary executive theory and is an important facet of effective government.

However, when the OSC does demand production of all privileged documents, then that encroaches on executive deliberations and decision-making. Executive privilege is "inextricably rooted in the separation of powers under the Constitution"[209] and has been judicially recognized and utilized by Presidents since the founding.[210] It is not something that can just be legislated away, as we discussed in Part II(c) by looking at how the Supreme Court has analyzed issues of Presidential and executive immunity in the face of statutes providing for civil damages

remedies.[211] Congress cannot just create rights of action, or in the alternative statutorily abrogate executive privileges that are rooted in the Constitution. Just because Congress created the OSC does not mean Congress can constitutionally maintain control over executive functions carried out by the agency,[212] which would include controlling executive decision-making.

To say that Congress can control, or even legislate away, constitutionally based foundational principles that protect executive decision-making would encroach on the executive branch by forcing its discussions to be subject to public and congressional scrutiny. Admittedly, the privileges are not spelled out in the Constitution, but they have operated in gaps for centuries and have been judicially recognized. If Congress did not agree with or recognize these fundamental rights, they should have expressed so long ago. As we learn in *Midwest Oil*, congressional acquiescence may provide support for executive action, even in the face of a statutory restriction.[213] If Congress wanted to question the existence of the privilege, it should have lodged the objection to the privilege as a whole when George Washington refused to produce the documents pertaining to the Jay Treaty.[214] Instead, by simply acknowledging the privilege and challenging the application of it, Congress acquiesced to its existence and courts have reinforced its importance.

Congress is also not limitless in its ability to pass laws of general applicability.[215] There is no enumerated power giving Congress the power to legislate over privileges claimed by executive branch employees. One may point to *Nixon v. Administrator of General Services*[216] to argue for congressional control over executive material, but information obtained for the public's knowledge and understanding of historical events and governmental preservation of those events is markedly different from information obtained as part of an adversarial investigation that could end up in a prosecution.

Even under the test of *Nixon v. Administrator of General Services*, which is described in section II(d)[217], the OSC Reauthorization Act of 2017 disrupts executive decision-making by impacting the free flow of information and thereby reducing the quality of policy decisions. The inquiry then turns to whether that disruption is justified by promoting objectives within the constitutional authority of Congress. Congress's general interest in oversight is not enough. Its interest in the *Nixon* case was much stronger because Congress had specific needs to preserve certain material for governmental and historical use. Congress provides no specific examples where executive privilege has been used to shield wrongdoing, and Congress can still conduct oversight with non-privileged material. Without any specific information about why it needs privileged information to conduct oversight, the executive branch's constitutionally based privileges must

prevail. It is clearly an overreach of Congress to say the executive must turn over all privileged material with no limiting principle.

Additionally, the President has "enhanced responsibility" to resist unconstitutional provisions that encroach on powers of the presidency.[218] Particularly considering the constitutional law considerations of "acquiescence" and "customs," there is a sense that an actor may lose it if they do not use it, so to say. Under the Take Care clause[219] and the President's oath of office, his constitutional duty is to protect and defend the constitutionally rooted doctrine of executive privilege. The President cannot faithfully execute a law that abrogates a power of his or her office that has constitutional dimensions and has been implicitly recognized and reinforced with centuries of congressional acquiescence.

Admittedly, the fact that the President signs a bill into law without exercising his or her veto power does not weigh in his or her favor. But, a 1994 OLC opinion speaking to the President's authority to decline to execute unconstitutional statutes argues the fact a sitting President signed the statute in question does not change the analysis.[220] Especially considering the size of bills today, it is often the case that a President signs a bill so the government will continue to function, though he believes part of that same bill is unconstitutional.[221] It would be a dangerous proposition to contend that the act of signing a bill with thousands of provisions renders any objections or interpretations not held at the time of signing invalid. It would also be a dangerous proposition to say that one Chief Executive's decision regarding constitutionality would bind the executive branch in perpetuity, despite the continuously changing nature of government.

While this article maintains that the unconstitutional provision regarding privileges in the OSC Reauthorization Act of 2017 should be resisted, the recommendation for executive officials to refuse to turn over the information should specifically be at the direction of the Chief Executive. While it may seem intuitive, it is worth addressing why it must be at his or her command. The founders intentionally divided the legislative branch due to its enormous powers to enact legislation;[222] however, they created a unitary executive where all of the executive power is vested in the Chief Executive.[223] The framers would likely be surprised to find that in modern government, there is an unprecedented amount of conflict *within* the executive branch that erodes the efficient operation of our government, as is the issue presented here.

Although the OSC does present welcome conflict intrabranch when it "kills the viruses" per the earlier analogy, its existence also inevitably creates division. The more the executive divides itself, the more difficult it is to hold any one actor

accountable.[224] As Steven Calabresi notes, plurality defeats accountability.[225] The OSC accessing privileged material that may aid in the prosecution of an intra-branch agency is more indicative, in Steven Calabresi's words, of an "executive power cartel."[226] As he notes, this may be more dangerous than a "unitary executive monopolist."[227] This is particularly ironic when an "executive power cartel" like the OSC was established to ferret out executive wrongdoing.

The intelligently designed executive division may yet illustrate another ulterior motive of Congress. Congress creates independent executive agencies by statute. Interestingly, as Steven Calabresi notes, the more the executive is divided, the greater the opportunity for state and local governments to operate in the gaps created by that division.[228] When the executive is unable to serve as a national check, then special interests win.[229] When conflicts between facets of the executive branch and the OSC drain too much time and energy, that detracts from the united front envisioned by the framers. To say this may have been anticipated by Congress may be cynical but must be considered. The President, as the brain of the executive body, must control this division by expressing a united front on his decisions regarding executive privilege, and by ensuring his subordinates are carrying out those wishes.

However, as alluded to previously, protecting privileged documents that are truly privileged does not mean that the executive refuses to compromise on communications that are not privileged—particularly when disclosure would not harm executive functions but may in fact assist with maintaining equilibrium in government. The executive should have a will of its own, but should equally respect the other two branches working in pursuit of their assigned functions. This means that once you remove the white blood cells that attack the healthy tissue, you leave the rest of the white blood cells intact to continue to attack viruses.

The provision requiring privileged material be turned over the OSC should also not be followed because the agency must consistently assert privilege to maintain it in other settings. The biggest take-away from *Coastal Gas* and *Mead Data* is that the agency must take steps to maintain the confidentiality of the privileged documents for a claim of privilege to be recognized. The *Fast and the Furious* case demonstrates that cooperation with an independent executive agency can diminish the agency's right to claim privilege to that information. Given the OSC actually compares itself to the IG in reference to its power to obtain privileged information,[230] executive agencies are right to be concerned that disclosures made to the OSC may be further released to Congress or even the public through the various reporting and disclosure practices and policies that agencies employ.

Additionally, given the extensive reporting requirements of the OSC to Congress and the fact that many of the OSC reports are publicized, the OSC Reauthorization Act of 2017 unconstitutionally encroaches on the executive by providing them access to privileged executive information. Information disputes between the legislative and executive branch have a substantial history[231] with both branches being particularly sensitive about legislative access to executive branch information.[232] President Jackson wrote that if Congress could point to a case suggesting corruption or abuse of trust, he would open up the entirety of the executive branch to them.[233] However, the OSC wants to reverse this view. In its estimation, they want everything provided to them and then they will point to the corruption. This approach completely ignores the intelligently designed institutional competition between the executive branch and independent agencies that report to the legislature, and encroaches on the executive deliberative process.

The other issue with this approach is that it diminishes any future claim of privilege for the agency. The executive branch cannot just divulge everything and then expect that its privilege claim will stand on the same footing as if it had never revealed the information to begin with, as illustrated in the *Fast and Furious* case. The OSC is a statutorily created conduit for providing executive information to Congress. Not only are the reporting requirements extensive, but the failure to recognize common law privileges provides the OSC with a blank check for information to aid in prosecution. When the prosecution comes to bear, Congress will certainly be able to ascertain the information underlying the proceeding. The institutional competition between the executive and Congress was by design. It upsets the balance of powers and the necessary gridlock if Congress can, through the conduit of an independent executive agency, access the advice executive agencies receive from their attorneys, particularly when it is deliberative.

The court in *Mead Data* protected discussions between agency personnel about the merits of various positions that could be adopted in contract negotiations.[234] This would certainly extend to various positions an agency could take in a labor or employment dispute. While *Mead Data* admittedly dealt with disclosure to the public, its rationale does not just disappear because the seeker of the information is an adversarial independent agency that reports extensively to Congress. In fact, Congress is not only elected by the public, but most of its reports and debates are public.[235] Of course agency officials will feel uncomfortable providing extensive information to their attorneys if they know may end up in Congress's hands. Additionally, the information seeker in the *Fast and the Furious* saga was Congress, and the court still found the deliberative process applied to documents reflecting the Department's internal deliberations about how to respond to Congressional and media inquiries about Operation Fast and Furious. If the framers truly intended

Congress and the executive to share all of their information, including privileged information, then why separate them at all?

Critics may point to the fact that executive privilege may be overused to shield wrongdoing. First, despite the power of the executive to make a privilege decision, Congress does have some tools it can utilize to attempt to control the executive. Admittedly, the tools are not extremely effective (hence the fact executive privilege is so controversial) but they are available for Congressional use. Some of these tools include issuing subpoenas, restricting funding, filing resolutions of inquiry, impeachment, and conducting oversight investigations.[236] Second, history bears out that executive privilege has largely not been used without a rational basis to do so.[237]

There is also no settled practice of giving Congress whatever it wants from the executive branch.[238] What history has shown is that there has typically been a good faith effort on both Congress and the executive branch to negotiate these disputes.[239] However as mentioned previously, it has not been the policy of the Trump Administration to negotiate these disputes.[240] The next section of this article recommends that the spirit of compromise be resurrected and the parties create an independent commission to conduct an impartial review based on agreed upon standards of the law of privilege. Cooperation is essential to finding the optimal solution for both parties and may even have constitutional undertones.[241] If the executive follows the advice of this article and stops handing over privileged information to the OSC, then the OSC can pursue a court-monitored settlement to try to coerce compliance. However, that could take years, assuming that a court finds it is even justiciable. For all of these reasons, the compromise this article proposes next is the best method to evaluate the differing needs of the parties, based on mutually agreed upon standards, in hopes of finding the optimal accommodation.

B. Proposal for a Privilege Review Commission

In the *McGahn* case, the court noted that judicial intervention in interbranch disputes would displace the historical practice of negotiation between the branches.[242] The court failed to address the role of the courts when negotiation is not a viable option. Efforts to negotiate have been replaced with executive defiance in the Trump Administration. The impeachment trial of President Trump highlighted how powerless and incapable Congress really is when the executive branch can define the scope of its own privilege, even when Congress is requesting information to fulfill its constitutional duty of impeachment. Rather than waiting years for a court to assist with the delicate and sensitive issue of executive privilege, this article recommends that the OSC, Congress, and the executive branch reach an agreement

to establish a privilege review commission (PRC). The PRC will be limited to reviewing privilege claims in the context of OSC investigations. First, it should be noted that this proposal is contingent on the OSC, and by extension Congress, refusing to agree to seek repeal of the provision regarding the OSC's access to privileged material. Second, the proposal is contingent on either a court declining to hear the issue; or the legal dispute taking so long that an interim solution is required. Finally, this commission only applies to executive agency claims of privilege in the context of OSC investigations. The sensitive and delicate decisions regarding privilege in other areas would not be subject to review by the PRC.

Based on former Special Counsel Lerner's testimony on agency claims of attorney-client privilege, the OSC's primary objection to agency claims of privilege was that agencies were using claims of privilege to shield non-privileged and relevant information. The PRC would help alleviate the fears Special Counsel Lerner discussed because the review would be conducted by an impartial panel and decisions would be based on mutually agreed upon standards of privilege. Additionally, the commission would also benefit the executive agencies because as compared to the current solution (where the OSC declines to recognize any privilege whatsoever), at least the PRC would protect agency materials that truly are privileged.

The most obvious issue is whether a recommendation for a commission of this sort contradicts Part III(A) of this article, which heralds the Chief Executive as the head of a united branch. First, this commission is not designed to decide claims of executive privilege outside of the context of OSC investigations. Thus, the President will still be able to utilize privilege as to other sensitive matters, such as national security and foreign affairs. Second, returning to the analogy of the executive branch as the human body, the President as the brain, and the OSC as the white blood cells. The OSC, when it kills the viruses, is a healthy part of the equilibrium of the body and for the large part, fits in with the unitary executive. When it seizes privileged material, akin to attacking the healthy tissue, it falls outside of the united front. This commission will help achieve that equilibrium and bring the executive branch back into balance.

In fact, some may say that with the strategies of the current administration, such a commission is necessary to maintain equilibrium because the President, as opposed to the OSC, still has too much power. As mentioned in part II(C), there has never been such a broad-scale defiance of requests for congressional information in the history of the republic than with the President's refusal to provide information in response to congressional requests for information.[243] While executive privilege has not been historically misused,[244] the Trump Administration has

been unprecedented in its defiance. There is nothing stopping the administration from withholding documents from the OSC and then refusing to compromise or budge from its refusal. The PRC would not permit executive defiance and would therefore alleviate concerns about broad-scale claims of executive privilege in the face of legitimate congressional or independent agency demands. As described below, the decision on disclosure is with the commission based upon the mutually agreed upon guidelines. Congress is also yearning for some sort of independent verification of privilege claims, as indicated by the *AT&T*[245] decision. The PRC will provide that.

Even though the PRC proposal is only in the context of OSC investigations, it is still of utmost importance to make sure that when you are making a recommendation of great import to the institution of the presidency and the executive as a whole, that you consider the implications to each and every President that will come to serve our nation. Although it is tempting to make changes based on behavioral idiosyncrasies of individual Presidents, the goal is to search for neutral principles of general applicability that will stand the test of time. Along those lines, it would not be appropriate to stand up a commission only because of the way a certain administration handles separation of powers issues. If the commission is established, it will apply to assertions of privilege in OSC investigations under both Republican and Democratic administrations. One must understand and accept decisions of the commission, even when it may not comport with a desired political outcome. However, pointing back to the relatively infrequent assertions of executive privilege that could not come to a negotiated solution in our nation's history;[246] this infrequency shows that the PRC may not have to be involved as often as one may surmise. The potential of the commission's intervention may even quell claims of privilege in favor of negotiation.

Given the general need for a commission, one of the foremost issues to be addressed is under which branch of government the PRC would be lodged. Under *Bowsher v Synar*, Congress cannot retain control over officers that are performing executive functions.[247] Additionally, the legislature writes laws of general applicability. It would not be appropriate for someone falling under the legislature to make individualized determinations on privileges asserted by the executive branch. Further, the judiciary is not appropriate because the inherently political work of the privilege review commission may undermine public confidence in the independence of judges.

In *Mistretta v. United States*, the Supreme Court upheld a sentencing commission lodged in the judicial branch and comprised of members appointed by the President and subject to removal by the same for neglect of duty, malfeasance, or other

good cause.[248] A voting member serves for six years and cannot serve more than two terms.[249] At least three of the members were to be federal judges.[250] The commission's duty was to establish "determinative sentencing guidelines."[251] The Court found that the ultimate question is whether a particular extradjudicial assignment undermines the integrity of the judicial branch and held that the sentencing commission did not.[252] The court also found that the President's appointment and removal authority over the members did not give him authority over the judicial branch or undue sway over its members.[253] Although the court in *Mistretta* upheld the commission, the court gave the most credence to petitioner's argument that because the commission would be working on a political issue, it would undermine the public confidence in the "disinterestedness" of judges.[254]

The PRC would handle an issue that is arguably more entangled in politics than sentencing. Decisions on privileges claimed by the executive are extremely newsworthy and often controversial. To have a judge be the ultimate arbiter of a claim of executive privilege may cause the public to believe he supports or does not support the President's political party, even if the decision was actually made impartially by the judge. The court in *Mistretta* noted that not all extrajudicial assignments would be appropriate[255] and serving on a privilege review commission would likely fall into that category.

That leaves the executive branch, which would be the most appropriate place for the privilege review commission, particularly because it would be handling claims of privilege asserted by the executive branch (thus carrying out an executive function). Before one balks at the idea of Congress agreeing to this construct, note that most of the agencies created by Congress that are "independent" fall under the executive branch. This includes the OIG and the OSC.[256] The PRC would be similarly situated. Like the OIG and OSC, its members would be appointed by the President and subject to removal for inefficiency, neglect of duty, or malfeasance in office, therefore providing some measure of independence. The ideal member would be someone with legal training who is independent of both agencies. No more than three members could come from the same political party.

An agency's structure and the substantive delegations of authority granted to it impact how much control presidents have over an agency.[257] This is why it is of the utmost importance that the substantive delegations to the agency carefully outline the agreement between all parties. The PRC would review the material claimed to be privileged and apply the law of privilege as agreed upon by all parties. Upon the PRC's findings, the privileged documents would be withheld or the privileged portions redacted, and the non-privileged information would be turned over to the OSC. A non-disclosure agreement would apply to all members

of the commission with regards to all material they review. Members of the commission would be subject to discharge from their duties if the non-disclosure agreement is violated; helping to assuage agency concerns over leaks to Congress or the public.

To be clear, this commission would not preclude judicial intervention. In fact, decisions of the commission should be appealable to federal district court. It is important for there to be an appealable avenue to the highest court in the land because of the potential that a decision of the commission is in conflict with that of the President. In addition, as discussed in Part II, in some circumstances it is proper for courts to rule on the scope of executive privilege.[258] However, if judicial review is sought for a decision of the PRC, the PRC's decision should apply in the interim.

Finally, the PRC would provide the public with some assurance that the process is fair. Individuals that have been wronged in the workplace deserve a full and fair investigation and prosecution. The agency and its officials also deserve a full and fair investigation where their right to receive confidential legal advice is respected. The balance has been upset with the passing of the OSC Reauthorization Act of 2017 and the PRC will help correct the current imbalance. The PRC would help the executive branch sort through its own documents to legitimately claim privilege, while simultaneously reassuring independent agencies and Congress that the claims are getting a second look under mutually agreed upon guidelines.

IV. Conclusion

It is in the public interest for agency officials to receive confidential legal advice. Particularly with regard to labor and employment decisions, agency officials must feel free to weigh and discuss all of their options and not be "forced to operate in a fishbowl."[259] Without access to privileged information, the OSC will still be able to conduct investigations, interview witnesses, and obtain all relevant non-privileged information for its report. While the OSC would prefer a blank check, so would any prosecuting body. However, the system as it is designed is a system that prioritizes the free flow of information between agency attorneys and agency officials. This free flow of information is a particularly important tenet in the adversarial process, which certainly includes an OSC investigation that can end in prosecution.

The OSC Reauthorization Act of 2017 unconstitutionally aggrandizes Congress and unconstitutionally encroaches on the executive. It provides Congress with a conduit (the OSC) to obtain information about the inner-workings of the executive deliberative process. There are no statutory or regulatory guarantees that the

privileged information obtained by OSC will not flow to third parties—the OSC only promises agency "consultation" before distribution, not agency approval. The OSC works very closely with Congress and is required to report to it on matters when requested. The OSC Reauthorization Act of 2017 also allows Congress to legislate away a judicially recognized and constitutionally based privilege. The President has a duty to prevent this sort of encroachment on executive decision-making. For these reasons, the executive should immediately stop turning over privileged material to the OSC at the direction of the President. The OSC, Congress, and the executive should revive the spirit of compromise, and come to the optimal accommodation of independent review for claims of privilege. An independent review will allow the OSC to receive independent verification of executive agency claims of privilege while also respecting the right of the agency to receive confidential legal advice.

Endnotes

[1] About OSC, Office of Special Counsel, https://osc.gov/Agency (last visited March 2, 2020) (noting that the OSC is an independent federal investigative and prosecutorial agency).

[2] *Id.*

[3] *See* 5 U.S.C. § 1212 (2017).

[4] *Transparency at TSA: Hearing Before the H. Comm. on Oversight and Gov't Reform*, 115th Cong. 31-35 (March 2, 2017) [hereinafter *Hearings*] (statement of Special Counsel Carolyn N. Lerner, Office of Special Counsel); *see also* Frequently Asked Questions: OSC Access to Privileged Materials, Office of Special Counsel, https://osc.gov/Resources/Pages/Policies.aspx (last visited March 2, 2020).

[5] *Id.*

[6] 5 U.S.C. § 1212(b)(5)(C)(i)(2017).

[7] Frequently Asked Questions: OSC Access to Privileged Materials, Office of Special Counsel, https://osc.gov/Resources/Pages/Policies.aspx (last visited March 2, 2020).

[8] *See* Whitehouse v. United States Dist. Court, 53 F.3d 1349, 1360 (1st Cir. 1995) (explaining it is necessary to the foundation of our adversarial system that clients feel comfortable giving information to attorneys) (citing 1 *McCormack on Evidence* § 87, at 316-17 (4th ed. 1992); Max D. Stern & David Hoffman, *Privileged Informers: The Attorney Subpoena Problem and a Proposal for Reform*, 136 U. Pa. L. Rev. 1783, 1826-27 (1988)).

[9] Lory Barsdate, *The Republican Civic Tradition: Attorney-Client Privilege for the Government Entity*, 97 Yale L.J. 1725, n.1 (1988) ("The classic formulation extends the attorney-client privilege in the following situation: (1) where legal advice of any kind is sought (2) from a professional legal advisor in his capacity as such, (3) the communications relating to that purpose, (4) made in confidence (5) by the client, (6) are at his instance permanently protected (7) from disclosure by himself or by the legal advisor, (8) except when the protection is waived) (citing 8 J. Wigmore, Evidence in Trials at Common Law § 2292, at 554 (J. McNaughton rev. ed. 1961)).

[10] Frequently Asked Questions: OSC Access to Privileged Materials, Office of Special Counsel, https://osc.gov/Resources/Pages/Policies.aspx (last visited March 2, 2020).

[11] Paul C. Light, Monitoring Government: Inspectors General and the Search for Accountability 39 (The Brooking Institution, 1993).

[12] *See generally id.*

[13] Comm. on Oversight & Gov't Reform v. Lynch, 156 F. Supp. 3d 101 (D.D.C. 2016).

[14] Although the Court mentioned that the DOJ chose to release the report, it is standard practice for the DOJ OIG to publish its reports. *See* Reports, Office of the Inspector General Department of Justice, https://oig.justice.gov/reports/all.htm. It is not as if this one report was selected for publication to prove innocence; in fact, the DOJ was heavily criticized as a result of the publication of the Fast and the Furious report. *See* Kevin Cirilli, *Report: IG Rips on DOJ in Fast and Furious*, Politico (September 11, 2012), https://www.politico.com/story/2012/09/report-ig-rips-doj-on-fast-furious-081044; Terry Frieden, *'Fast and Furious' Report Slaps 14 at Justice, ATF*, CNN (September 19, 2012), https://www.cnn.com/2012/09/19/us/us-fast-furious-report/index.html.

[15] *Comm. on Oversight v. Lynch*, 156 F. Supp. 3d at 114.

[16] *See* Mead Data Cent., Inc. v. United States Dep't of the Air Force, 566 F.2d 242, 253 (D.C. Cir. 1977) (it must be established that the information is confidential for the privilege to apply); Coastal States Gas Corp. v. Dep't of Energy, 617 F.2d 854, 863 (D.C. Cir. 1980) (finding the privilege was not available to the agency for some documents because the agency "failed to demonstrate a fundamental prerequisite to assertion of the privilege: confidentiality both at the time of the communication and maintained since").

[17] *Presidential Authority to Decline to Execute Unconstitutional Statutes*, 18 Op. O.L.C. 199, 201 (1994).

[18] *Compare* President Ronald Reagan, Memorandum for the Heads of Executive Departments and Agencies for Procedures Governing Responses to Congressional Requests for Information, H.R. Rep. No. 435, 99th Cong., 1st Sess. 1106 (1985) (declaring the "tradition of accommodation should continue as the primary means of resolving conflicts between the branches") *with* Jonathon Shaub, '*Masters from Two Equal Branches of Government': Trump and Congress play Hardball*, Lawfare (April 27, 2019), https://www.lawfareblog.com/masters-two-equal-branches-government-trump-and-congress-play-hardball (noting that the Trump Administration has proclaimed they will fight "all the subpoenas").

[19] The United States Dep't of Justice, FOIA Update, Vol. VI, No. 2 (January 1, 1985), https://www.justice.gov/oip/blog/foia-update-oip-guidance-attorney-client-privilege.

[20] Anne Tindall & Jessica Marsden, *What Independent Investigations of the Past can Teach Us About the Mueller Probe*, Lawfare (January 11, 2019, 8:06 AM), https://www.lawfareblog.com/what-independent-investigations-past-can-teach-congress-about-its-role-mueller-probe.

[21] *Id.*

[22] Ken Gormley, *The Saturday Night Massacre: How Our Constitution Trumped a Reckless President*, National Constitution Center (October 20, 2015), https://constitutioncenter.org/blog/the-saturday-night-massacre-40-years-later-how-our-constitution-trumped-a-r.

[23] *Id.*

[24] *Id.*

[25] *Id.*

[26] *Id.*

[27] *Id.*

[28] *See generally* Tiffany R. Murphy, *Prosecuting the Executive*, 56 San Diego L. Rev. 105 (2019).

[29] *See generally* discussion *supra* note 14.

[30] *Id.*

[31] Ethics in Government Act of 1978, P.L. 95-521, §§ 601-04, 92 Stat. 1824, 1867-75.

[32] Pub. L. No. 95-454, 92 Stat. 1111 (1978) (codified as amended predominantly in scattered sections of 5 U.S.C.).

[33] Morton Rosenberg, *Separation of Powers and the Executive Branch: The Reagan Era in Retrospect: Congress's Prerogative Over Agencies and Agency Decisionmakers: The Rise and Demise of the Reagan Administration's Theory of the Unitary Executive*, 57 Geo. Wash. L. Rev. 627, 662 (1989).

[34] About MSPB, Merit Systems Protection Board, https://www.mspb.gov/About/about.htm (last visited 3 March 2020).

[35] *Id.*

[36] Rosenberg, *supra* note 33, at 666 (citing 5 U.S.C. § 1211, 134 Cong. Rec. S15, 330).

[37] 5 U.S.C. § 1211(b) (1989).

[38] *Id.*

[39] *See generally* Kirti Datla and Richard L. Revesz, *Deconstructing Independent Agencies (And Executive Agencies),* 98 Cornell L. Rev. 769, 772 (2013).

[40] Rosenberg, *supra* note 33, at 668.

[41] *Id.*

[42] *See* Bowsher v. Synar, 478 U.S. 714, 734 (1986) (holding it was unconstitutional for Congress to retain removal power over officer performing executive functions) *and* Myers v. United States, 272 U.S. 52, 176 (1926) (the President has unrestricted powers of removal over the postmaster general).

[43] Morrison v. Olson, 487 U.S. 654, 696-97 (1988).

[44] *See* 5 U.S.C. § 1211(b) (1989) (The Special Counsel may be removed by the President only for inefficiency, neglect of duty, or malfeasance in office).

[45] *Morrison v. Olson*, 487 U.S. at 694.

[46] *Id.*

[47] Office of Special Counsel, Policy Statement on Disclosure of Information from OSC Program Files (2004), https://osc.gov/Documents/PPP/Policy%20Statements/Policy%20Statement%20on%20Disclosure%20of%20Information%20from%20OSC%20Program%20Files.pdf.

[48] *Id.*

[49] 5 U.S.C. § 1217(a) (1989) (emphasis added).

[50] Testimonies and Transcripts, Office of Special Counsel, https://osc.gov/Resources/Pages/Testimonies.aspx.

[51] *Hearings* (statement of Special Counsel Carolyn N. Lerner, Office of Special Counsel), *supra* note 4.

[52] S. Rep. No. 115-74 (2017).

[53] *Id.*

[54] *See Hearings* (statement of Special Counsel Carolyn N. Lerner), *supra* note 4.

[55] *Hearings* (statement of Special Counsel Carolyn N. Lerner, Office of Special Counsel) *supra* note 4, at 32.

[56] *Hearings* (statement of Special Counsel Carolyn N. Lerner, Office of Special Counsel) *supra* note 4, at 32-33.

[57] *See* Upjohn Co. v. United States, 449 U.S. 383, 389 (1981); *see also* Grace M. Giesel, *The Legal Advice Requirement of the Attorney-Client Privilege: A Special Problem for In-House Counsel and Outside Attorneys Representing Corporations,* 48 Mercer L. Rev. 1169, 1184 (1997).

[58] 5 U.S.C. § 552 (2016).

[59] Dep't of Justice Guide to the Freedom of Information Act, Department of Justice (2019), https://www.justice.gov/oip/foia-guide/introduction/download.

[60] *Id.* at 1 (citing NLRB v. Robbins Tire & Rubber Co., 437 U.S. 214, 242 (1978)).

[61] *Id.* at 2.

[62] *Id.* (citing John Doe Agency v. John Doe Corp., 493 U.S. 146, 152 and Dep't of the Air Force v. Rose, 425 U.S. 352, 361 (1976) (holding that "limited exemptions do not obscure the basic policy that disclosure, not secrecy, is the dominant objective of the Act").

[63] 5 U.S.C. § 552(b)(5).

[64] Coastal States Gas Corp. v. Dep't of Energy, 617 F.2d 854, 862 (D.C. Cir. 1980) (noting "the courts have recognized that Exemption 5 protects, as a general rule, materials which would be protected under the attorney-client privilege; the attorney work-product privilege; or the executive 'deliberative process' privilege" (internal citations omitted)).

[65] *Id.* at 863.

[66] *Id.* at 870.

[67] *Id.* at 863.

[68] *Id.*

[69] *Id.* at 864.

[70] Mead Data Cent., Inc. v. United States Dep't of the Air Force, 566 F.2d 242 (D.C. Cir. 1977).

[71] *Id*. at 249.

[72] *Id.* at 252.

[73] *Id.*

[74] *Id.*

[75] *Id.* at 253-54.

[76] Mead Data Cent., In. v. United States Dep't of the Air Force*,* 566 F.2d 242, 262-63 (D.C. Cir. 1977).

[77] Coastal States Gas Corp. v. Dep't of Energy, 617 F.2d 854, 862 (D.C. Cir. 1980).

[78] Mead Data 566 F.2d at 256 (citing S. Rep. No. 813, 89th Cong., 1st Sess. 9 (1965); H.R. Rep. No. 1497, 89th Cong., 2d Sess. 10 (1966); Katz, *Games Bureaucrats Play – Hide and Seek Under the Freedom of Information Act*, 48 Tex. L. Rev. 1261, 1272-77 (1970); Comment, *The Freedom of Information Act and Its Internal Memoranda Exemption: Time for a Practical Approach*, 27 Sw. L.J. 806 (1973)).

[79] *See* Model Rules of Prof'l Conduct r. 1.6 (Am. Bar. Ass'n 1983) (lawyers may have a duty to disclose information that the lawyer believes necessary to "to prevent the client from committing a crime or fraud that is reasonably certain to result in substantial injury to the financial interests or property of another and in furtherance of which the client has used or is using the lawyer's services;" *see also* Model Rules of Prof'l Conduct r. 8.4 (it is professional misconduct for a lawyer to engage in conduct involving dishonesty, fraud, deceit or misrepresentation).

[80] *See* Model Rules of Prof'l Conduct r. 1.6.

[81] Kerri Blumenauer, *Privileged or Not? How the Current Application of the Government Attorney-Client Privilege Leaves the Government Feeling Unprivileged*, 75 Fordham L. Rev. 75, 80 (2006).

[82] Lieutenant Colonel Norman K. Thompson, USAF and Captain Joshua E. Kastenberg, USAF, *The Attorney-Client Privilege: Practical Application of a Professional Core Value*, 49 A.F. L. Rev. 1, 49 (2000).

[83] *Rethinking the Professional Responsibilities of Federal Agency Lawyers*, 115 Harv. L. Rev. 1170, 1178 (2002)(citing Michael Herz, *The Attorney Particular: Governmental Role of the Agency General Counsel, in Government Lawyers* 143, 147-50 (Cornell W. Clayton ed., 1995).

[84] *See generally* Restatement (Third) of the Law Governing Lawyers § 97 cmt. a (Am. Law Inst. 2000) (explaining that the duty of a lawyer representing a government entity is to "act in a manner reasonably calculated to advance the lawful objectives of the client entity as defined by persons authorized to instruct the lawyer on behalf of the client").

[85] *See* Thompson and Kastenberg, *supra* note 82, at 48.

[86] *See* Restatement (Third) of the Law Governing Lawyers, *supra* note 84.

[87] *See* discussion, *supra* note 9.

[88] *See* About OSC, *supra* note 1.

[89] Office of Special Counsel Reauthorization Act of 2017, Pub. L. No. 115-91 § 1097(a) (2017).

[90] *See Hearings* (statement of Special Counsel Carolyn N. Lerner, Office of Special Counsel), *supra* note 4.

[91] Public Files, Office of Special Counsel, https://osc.gov/PublicFiles.

[92] *Mead Data Cent., Inc. v. United States Dep't of the Air Force*, 566 F.2d 242, 253 (D.C. Cir. 1977).

[93] *Hearings* (statement of Special Counsel Carolyn N. Lerner, Office of Special Counsel), *supra* note 4.

[94] *See* U.S. v. Deloitte LLP, 610 F.3d 129 (D.C. Cir. 2010) (noting a limited disclosure to third parties is insufficient to waive the work product privilege, and that in order to waive the protection, the party must produce complete documents).

[95] *See Hearings* (statement of Special Counsel Carolyn N. Lerner, Office of Special Counsel), *supra* note 4.

[96] *See* Comm. On Oversight & Gov't Reform v. Lynch, 156 F. Supp. 3d 101, 113-115 (D.D.C. 2016).

[97] Public Files, Office of Special Counsel, https://osc.gov/PublicFiles.

[98] *Freedom of Information Act Exemption (5 U.S.C.A. § 552(b)(5)) for inter-agency and intra-agency memorandums or letters as applicable to communications to or from attorneys for the government*, 54 A.L.R. Fed. 280 (citing, among others, NLRB v. Sears, Roebuck & Co., 421 U.S. 132 (1975); NLRB v. Robbins Tire & Rubber Co., 437 U.S. 214 (1978); Coastal States Gas Corp. v. Dep't of Energy, 617 F.2d 854 (D.C. Cir. 1980)).

[99] *Hickman v. Taylor*, 329 U.S. 495 (1947).

[100] Marion J. Radson & Elizabeth A. Waratuke, *The Attorney-Client and Work Product Privileges of Government Entities*, 30 Stetson L. Rev. 799, 807 (2001).

[101] Hickman v. Taylor, 329 U.S. 495, 511 (1947).

[102] *Id.*

[103] Coastal States Gas Corp. v. Dep't of Energy, 617 F.2d 854, 864 (D.C. Cir. 1980).

[104] *See generally* Judicial Watch, Inc. v. United States DOJ, 118 F. Supp. 3d 266, 273 (D.D.C. 2015) (citing *Coastal Gas*, 617 F.2d at 864).

[105] 5 U.S.C. § 552(b)(5).

[106] *See generally*, *Freedom of Information Act Exemption (5 U.S.C.A. § 552(b)(5)) for inter-agency and intra-agency memorandums or letters as applicable to communications to or from attorneys for the governmen*t, 54 A.L.R. Fed. 280.

[107] NLRB v. Sears, Roebuck & Co., 421 U.S. 132, 154 (1975).

[108] *Id.* (citing S. Rep. No. 813, 89th Cong., 1st Sess. 9 (1965)).

[109] *Id.* (citing Kaiser Aluminum & Chemical Corp. v. United States, 157 F. Supp 939 at 947; United States v. Anderson, 34 F.R.D. 518 (Colo. 1963); Thill Securities Corp. v. New York Stock Exchange, 57 F.R.D. 133 (ED Wis. 1972); J. H. Rutter Rex Mfg. Co., Inc. v. NLRB, 473 F. 2d 223 (CA5), *cert. denied*, 414 U.S. 822 (1973)).

[110] *Id.* at 159-60.

[111] Kent Corp. v. NLRB*,* 530 F.2d 612 (5th Cir. 1976), *cert. denied*, 429 U.S. 920 (1976).

[112] *Id.* at 623-24.

[113] Coastal States Gas Corp. v. Dep't of Energy, 617 F.2d 854, 865 (D.C. Cir. 1980).

[114] *In re* Spec. Sept. 1978 Grand Jury, 640 F.2d 49, 64-65 n.19 (7th Cir. 1980).

[115] *See Freedom of Information Act Exemption, supra* note 98.

[116] *Coastal Gas*, 617 F.2d at 866.

[117] The Miller Center, Executive Privilege: Mapping an Extraordinary Power 6, http://web1.millercenter.org/reports/MC-executive-privilege.pdf [hereinafter *Executive Privilege: Mapping an Extraordinary Power*].

[118] *See* Nixon v. Adm'r of Gen. Servs., 433 U.S. 425, 509-10 (1977) (Burger, J., dissenting); Stephen Knott, *George Washington: Impact and Legacy*, UVA Miller Center (2019), https://millercenter.org/president/washington/impact-and-legacy.

[119] *See* Nixon v. Adm'r of Gen. Servs. at 509-10 (Burger, J., dissenting) (citing A. Bickel, The Morality of Consent 79 (1975); W. Taft, The Presidency 110 (1916)).

[120] *Executive Privilege: Mapping an Extraordinary Power, supra* note 117, at 48.

[121] *Executive Privilege: Mapping an Extraordinary Power, supra* note 117, at 43.

[122] *See generally* United States v. Nixon, 418 U.S. 683, 706 (1974)*;* Nixon v. Adm'r of Gen. Servs., 433 U.S. at 501 (Powell, J., concurring).

[123] Comm. On Oversight & Gov't Reform v. Lynch, 156 F. Supp. 3d 101, 109 (D.D.C. 2016) (citing *In re* Sealed Case, 121 F.3d 729, 736-37 (1997)).

[124] Jonathan Shaub, *The Executive's Privilege: Rethinking the President's Power to Withold Information*, Lawfare (October 31, 2019) https://www.lawfareblog.com/executives-privilege-rethinking-presidents-power-withhold-information.

[125] Jonathan Shaub, *Obstruction of Congress, Impeachment and Constitutional Conflict*, Lawfare (January 10, 2020) https://www.lawfareblog.com/obstruction-congress-impeachment-and-constitutional-conflict.

[126] Jonathan Shaub, *Testimony and Executive Privilege in the Senate Impeachment Trial*, Lawfare (January 15, 2020), https://www.lawfareblog.com/testimony-and-executive-privilege-senate-impeachment-trial.

[127] *See generally* Anderson v. Dunn, 19 U.S. 204, 231 (1821); Comm. on the Judiciary v. Miers, 542 F.3d 909, 911 (D.C. Cir. 2008).

[128] Comm. on the Judiciary of the United States House of Representatives v. McGahn, 951 F.3d 510 (D.C. Cir. 2020).

[129] 418 U.S. 683, 692 (1974).

[130] *Id.* at 708, 713.

[131] *Id.* at 708.

[132] 421 U.S. 132 (1975).

[133] *Id.* at 150.

[134] *Id.* at 150-52.

[135] *Id.* at 152-54.

[136] *Id.* at 153-54.

[137] Mead Data Cent., Inc. v. United States Dep't of the Air Force, 566 F.2d 242, 257 (D.C. Cir. 1977).

[138] *Id*. at 256.

[139] *Id*.

[140] *Id*.

[141] *See* Executive Privilege: Mapping an Extraordinary Power, *supra* note 117, at 54.

[142] *See* Executive Privilege: Mapping an Extraordinary Power, *supra* note 117, at 55.

[143] *See* Executive Privilege: Mapping an Extraordinary Power, *supra* note 117, at 48; *see also* U.S. Const. art. 1 § 3, cl. 6-7.

[144] INS v. Chadha, 462 U.S. 919, 951 (1983).

[145] *Compare Chadha*, 462 U.S. at 952 (majority opinion) (finding the house action was legislative in character and effect) *with Chadha*, 462 U.S. at 964 (Powell, J., concurring) (noting that he thinks the house action was "clearly adjudicatory").

[146] *See generally* Mistretta v. United States, 488 U.S. 361, 381 (1989).

[147] *Mistretta*, 488 U.S. at 380-81.

[148] 433 U.S. 425 (1977).

[149] *Id*. at 433.

[150] *Id*. at 442-43 (citing United States v. Nixon, 418 U.S. 683, 711-712 (1974)).

[151] *Id*.

[152] *Id*. at 454.

[153] *See generally Presidential Authority to Decline to Execute Unconstitutional Statutes*, 18 Op. O.L.C. 199, 200 (1994); *see also* Edwin M. Meese III, *The Law of the Constitution*, 61 Tul. L. Rev. 979, 985 (1987) (noting that determining the constitutionality of laws is the business of all three branches).

[154] Marbury v. Madison, 5 U.S. 137, 178-180 (1803).

[155] *See generally Presidential Authority to Decline to Execute Unconstitutional Statutes*, 18 Op. O.L.C. 199, 200 (1994).

[156] *See generally* Edwin M. Meese III, *The Law of the Constitution*, 61 Tul. L. Rev. 979, 985 (1987).

[157] *Compare Chadha*, 462 U.S. at 952 (majority opinion) (finding the house action was legislative in character and effect) *with Chadha*, 462 U.S. at 964 (Powell, J., concurring) (noting that he thinks the house action was "clearly adjudicatory").

[158] *See* Jacobellis v. Ohio, 378 U.S. 184, 197 (1964) (Stewart, J., concurring).

[159] Peter M. Shane, Harold H. Bruff & Neil J. Kinkopf, Separation of Powers Law 354 (Carolina Academic Press, 4th Ed. 2018).

[160] *Id.*

[161] *See* Executive Privilege: Mapping an Extraordinary Power, *supra* note 117, at 48-49.

[162] Tara Leigh Grove, *The Lost History of the Political Question Doctrine*, 90 N.Y.U. L. Rev. 1908, 1909 (citing Nixon v. United States, 506 U.S. 224, 228-29 (1993)).

[163] 369 U.S. 186, 217 (1962).

[164] United States v. Nixon, 418 U.S. 683, 708 (1974).

[165] *See* Comm. On Oversight & Gov't Reform v. Lynch, 156 F. Supp. 3d 101, 104-105, 119 (D.D.C. 2016); United States v. Nixon, 418 U.S. 683, 697 (1974).

[166] Comm. On Oversight v. Lynch, 156 F. Supp. 3d at 104 (citing United States v. Nixon, 418 U.S. 683 (1974)).

[167] *Id.* at 106.

[168] *Id.* at 110.

[169] *Id*. at 105.

[170] *Id.* at 114.

[171] *Id.*

[172] *See* discussion, *supra* note 14.

[173] 567 F.2d 121 (D.C. Cir. 1977).

[174] *Id.* at 123.

[175] *Id.*

[176] *Id.* at 124.

[177] *Id.* at 127.

[178] *Id.*

[179] United States v. Am. Tel. & Tel. Co., 567 F.2d 121, 130-133 (D.C. Cir. 1977).

[180] *Id.* at 127.

[181] 558 F. Supp. 2d 53 (D.D.C. 2008).

[182] *Id.* at 57-58.

[183] *Id.* at 57-62.

[184] *Id.* at 57-64.

[185] *Id.* at 63.

[186] *Id.*

[187] Comm. On the Judiciary v. Miers, 558 F. Supp. 2d 53, 63-64. (D.D.C. 2008).

[188] *Id.* at 107 (citing United States v. Nixon, 418 U.S. 683, 703-05 (1974); Marbury v. Madison, 5 U.S. 137, 177 (1803)).

[189] *Id.* at 103.

[190] *Id.* at 99.

[191] *Id.* at 106.

[192] *Id.* at 97.

[193] Comm. On the Judiciary v. Miers, 558 F.Supp. 2d, 98 (D.D.C. 2008).

[194] United States v. Am. Tel. & Tel. Co., 567 F.2d 121, 130-133 (D.C. Cir. 1977).

[195] Comm. on the Judiciary of the United States House of Representatives v. McGahn, 951 F.3d 510 (D.C. Cir. 2020).

[196] *Id.* at 537.

[197] *Id.* at 516 (citing *Marbury*, 5 U.S. at 170; *Raines v. Byrd*, 521 U.S. 811 at 834, Souther, J., concurring in the judgment).

[198] *Id.*

[199] *Id.* at 519.

[200] *Id.* at 520.

[201] *Id*. at 518.

[202] Josh Gerstein, *Full Appeals Court to Hear McGahn, Border Wall Cases,* Politico, March 13, 2020 https://www.politico.com/news/2020/03/13/appeals-court-don-mcgahn-border-wall-cases-128914.

[203] Michael Herz, *United States v. United States: When can the Federal Government Sue Itself?*, 32 Wm. & Mary L. Rev. 893, 910-11 (1991) (citing Buckley v. Valeo, 424 U.S. 1 (1976) (per curiam); Cheng Fan Kwok v. INS, 392 U.S. 206 (1968); United States v. Lovett, 328 U.S. 303 (1946)).

[204] *See id*. at 914 (explaining that the unitary executive would be viewed as a single person incapable of having a controversy with itself).

[205] One of the rationales underlying the *Humphreys* decision is that independent agencies engaged in quasi-legislative and quasi-judicial functions are not, and should not, be at the mercy of the Chief Executive. *See generally* Humphrey's Ex'r v. United States, 295 U.S. 602, 624 (1935) (explaining that the Commission is to be non-partisan and must act impartially).

[206] Myers v. United States, 272 U.S. 52, 135 (1926).

[207] 418 U.S. 683, 693 (1974).

[208] *Id.*

[209] United States v. Nixon, 418 U.S. 683, 708 (1974).

[210] *See* Executive Privilege: Mapping an Extraordinary Power, *supra* note 117.

[211] *See* Nixon v. Fitzgerald, 457 U.S. 731 (1982) (absolute immunity upheld for Presidential action in the outer perimeter of official action despite the fact that a statute provided otherwise); *see also* United States v. Reynolds, 345 U.S. 1 (1953) (even though statute and regulation supported the claim of parents of the victim in an Air Force bomber crash to the report, there was a valid claim of privilege that may prevent the victims from being able to exercise their statutory rights).

[212] *See* Bowsher v. Synar, 478 U.S. 714, 734 (1986) (holding it was unconstitutional for Congress to retain removal power over officer performing executive functions) *and* Myers v. United States, 272 U.S. 52, 176 (1926) (the President has unrestricted powers of removal over the postmaster general).

[213] *See* United States v. Midwest Oil Co., 236 U.S. 459, 474 (1915) (finding that a long-continued practice, known to and acquiesced in by Congress, would raise a presumption that the action had been "made in pursuance of its consent or of a recognized administrative power of the Executive in the management of the public lands").

[214] *See* Executive Privilege: Mapping an Extraordinary Power, *supra* note 117.

[215] *See* U.S. Const. art. I, § 8 (describing the categories of topics on which Congress can make laws).

[216] 433 U.S. 425 (1977).

[217] *Id.*

[218] *Presidential Authority to Decline to Execute Unconstitutional Statutes*, 18 Op. O.L.C. 199, 201 (1994).

[219] *See* U.S. Const. art. II, § 3 (the President shall take care that the laws be faithfully executed).

[220] *See* Nixon v. Adm'r of Gen. Servs., 433 U.S. 425, 443 (citing United States v. Nixon, 418 U.S. 683, 711-12 (1974)).

[221] *See* Peter M. Shane, Harold H. Bruff & Neil J. Kinkopf, Separation of Powers Law 146 (Carolina Academic Press, 4th Ed. 2018) (citing Peter M. Shane, Madison's Nightmare 132-42 (2016) (in his first six years in office, President George W. Bush lodged nearly 1400 objections to statutory provisions)).

[222] The Federalist No. 51 at 349 (James Madison) (Jacob E. Cooke ed., 1961).

[223] *See* U.S. Const. art. II, § 1 ("The executive power shall be vested in a President of the United States of America."); *see also* Myers v. United States, 272 U.S. 52, 117 (1926) (noting that not only was the vesting clause essentially a grant of power to execute the laws, but also comes with reasonable implications in carrying out that power, such as appointment and removal).

[224] Steven G. Calabresi, *Some Normative Arguments for the Unitary Executive*, 48 Ark. L. Rev. 23, 65 (1995).

[225] *Id*.

[226] *Id*. at 44.

[227] *Id*.

[228] *Id.* at 65.

[229] *Id.* at 65-66.

[230] Frequently Asked Questions: OSC Access to Privileged Materials, Office of Special Counsel, https://osc.gov/Resources/Pages/Policies.aspx (last visited March 2, 2020).

[231] Peter M. Shane, Harold H. Bruff & Neil J. Kinkopf, Separation of Powers Law 354 (Carolina Academic Press, 4th Ed. 2018) (citing Louis Fisher, the Politics of Executive Privilege (2004)).

[232] *Id.* at 354.

[233] *Id.* at 354-356 (citing Archibald Cox, *Executive Privilege*, 122 U. Pa. L. Rev. 1383, 1395-1405 (1974)).

[234] *See* Mead Data Cent., Inc. v. United States Dep't of the Air Force, 566 F.2d 242, 255 (D.C. Cir. 1977).

[235] For summaries of the daily congressional record, *see* Congressional Record, Congress.gov, https://www.congress.gov/congressional-record.

[236] *Congress's Authority to Influence and Control Executive Branch Agencies*, Congressional Research Service (updated December 19, 2018).

[237] *See generally* Archibald Cox, *Executive Privilege*, 122 U. Pa. L. Rev. 1383, 1395-1405 (reviewing the historical uses of executive privilege by past Presidents and finding that only two Presidents withheld information under circumstances where the withholding could not be easily justified).

[238] *Id*.

[239] *See generally* Reagan, Memorandum for the Heads of Executive Departments, *supra* note 18; *see also* Richard Lempert, *All the President's Privileges*, Brookings Institute (2019), https://www.brookings.edu/research/all-the-presidents-privileges/.

[240] *See* Reagan, Memorandum for the Heads of Executive Departments, *supra* note 18.

[241] United States v. Am. Tel. & Tel. Co., 567 F.2d 121, 127 (D.C. Cir. 1977) (negotiation may be considered a "constitutional mandate to seek optimal accommodation through a realistic evaluation of the needs of the conflicting branches in the particular fact situation").

[242] Comm. on the Judiciary of the United States House of Representatives v. McGahn, 951 F.3d 510 (D.C. Cir. 2020).

[243] Jonathan Shaub, *Obstruction of Congress, Impeachment and Constitutional Conflict*, Lawfare (January 10, 2020) https://www.lawfareblog.com/obstruction-congress-impeachment-and-constitutional-conflict.

[244] *See generally* Archibald Cox, *Executive Privilege*, 122 U. Ps. L. Rev. 1383, 1395-1405 (reviewing the historical uses of executive privilege by past Presidents and finding that only two Presidents withheld information under circumstances where the withholding could not be easily justified).

[245] United States v. Am. Tel. & Tel. Co., 567 F.2d 121, 124 (D.C. Cir. 1977) (noting that the stumbling block in negotiations between the legislative and executive branch over the subpoena was "the means of verifying the accuracy of the executive's classification of surveillance as domestic or foreign, and of the generic descriptions").

[246] *See generally id.*

[247] Bowsher v. Synar, 478 U.S. 714, 734 (1986) (holding it was unconstitutional for Congress to retain removal power over officer performing executive functions).

[248] Mistretta v. United States, 488 U.S. 361, 368 (1989).

[249] *Id.* at 368-69.

[250] *Id.* at 368

[251] *Id.* at 369.

[252] *Id.* at 404.

[253] *Id.* at 409.

[254] Mistretta v. United States, 488 U.S. 361, 407 (1989).

[255] *Id*. at 385.

[256] *See* About OSC, Office of Special Counsel, https://osc.gov/Agency (last visited March 2, 2020) (noting that the OSC is an independent federal investigative and prosecutorial agency); *see also* About the Office, U.S. Department of Justice Office of Inspector General, https://oig.justice.gov/about (last visited April 22, 2021) (noting that the OIG is a statutorily created independent agency).

[257] Kirti Datla and Richard L. Revesz, *Deconstructing Independent Agencies (And Executive Agencies),* 98 Cornell L. Rev. 769, 783 (citing Aziz Z. Huq, *Removal as a Political Question*, 65 Stan. L. Rev. 1, 25-32 (2013)).

[258] United States v. Nixon, 418 U.S. 683, 706 (1974) ("neither the doctrine of separation of powers, nor the need for confidentiality of high-level communications, without more, can sustain an absolute, unqualified Presidential privilege of immunity from judicial process under all circumstances"); Comm. on Oversight & Gov't Reform v. Lynch, 156 F. Supp. 3d 101, 113-114 (D.D.C. 2016) (judicial intervention appropriate because the facts are undisputed and negotiations have failed).

[259] Mead Data Cent., Inc. v. United States Dep't of the Air Force, 566 F.2d 242, 256 (D.C. Cir. 1977).

Continuous Evaluation and Credit Reports: Ensuring Fairness In Current Security Clearance Reforms

*Major Andrew H. Woodbury**

* Major Andrew Woodbury, USAF, (LL.M., The George Washington University Law School (2020); J.D., The George Washington University Law School (2014); B.A. Policy Studies and Public Relations, Syracuse University (2011)) is a litigation attorney presently assigned to the Air Force Labor Law Field Support Center, Personnel and Information Law Division, The Judge Advocate General's Corps. He is a member of the Pennsylvania bar. Major Woodbury would like to thank Professor Kel B. McClanahan for his assistance with this article.

I. Introduction

The security clearance process in the U.S. federal government is currently undergoing its biggest overhaul in over 50 years.[1] In March 2018, the Office of the Director of National Intelligence (ODNI) announced the inception of the Trusted Workforce 2.0 initiative with the goal of overhauling and improving the security clearance process, a framework that has been in place since the 1950s.[2] A key part of the initiative to modernize a security clearance process badly in need of an update is the use of "Continuous Evaluation" (CE).[3] CE allows federal agencies to get a "near-real-time look" at its employees. It can alert agencies to "potential red flags on a clearance holder's credit or financial transactions" or search for "suspicious transactions, foreign travel or potential links to terrorism."[4] "The trustworthiness of those who guard the secrets of the [U.S.] should be beyond reproach" and using advances in technology to improve the system used to assess the trustworthiness of clearance holders is a necessary development.[5] Although "insider threats" are not new, the past decade has seen multiple high profile examples of government insiders attacking fellow workers and unlawfully disclosing national security information. "[T]hreats such as Chelsea Manning and Edward Snowden (trusted insiders who stole and released classified data) and U.S. Army Major Nidal Hasan (who killed 13 and injured more than 30 at Fort Hood, Texas)" provided the momentum needed to bring the security clearance and vetting process into the current era.[6] Not only could CE help identify insider threats sooner, but it could also reduce the costs associated with the security clearance process and help reduce the backlog of security clearances currently pending for periodic reinvestigation.[7]

However, with every technological innovation comes tradeoffs and new challenges. CE will rely on automated records checks of "commercial databases, Government databases, and other information lawfully available to security officials."[8] These "commercial databases" include consumer credit information from credit reporting agencies.[9] Credit reporting agencies have been criticized or allowing inaccuracies to pervade the consumer credit reports of millions of Americans.[10] In many ways, "large scale inaccuracies are tolerated" by credit bureaus because they "have little economic incentive to conduct proper disputes," improve their investigation, or prevent erroneous information from appearing in credit reports.[11] The use of credit reports and consumer credit information in the security clearance process is not new, but the use of real-time automated record checks and other technological innovations may exacerbate existing problems with the security clearance investigation process and create new problems.

This article recommends several policies that could help alleviate some of these problems. Part II of this article explains how government employees and contractors gain and retain eligibility to access classified information, discusses problems with the security clearance process, and describes current ongoing changes to the process. Part III discusses CE, how it is being implemented across the federal government, and how it uses consumer credit information. Part IV explains how the consumer credit reporting industry operates and how it is regulated. It also discusses several critiques of credit reporting agencies and unfair debt collection practices. Lastly, Part V discusses several policy proposals that would alleviate some of the concerns from using consumer credit information in an automated CE process. There are several ways the ODNI can protect current clearance holders from the effects of erroneous or misleading consumer credit information: (1) mandate an effective, centralized investigation database that prevents the reflagging of previously adjudicated issues in credit records; (2) ensure appropriate oversight and burden sharing among agencies, credit reporting agencies, and clearance holders; (3) require the reporting and analysis of automated records check systems to identify potential bias or disparate impacts on protected classes and minority groups; and (4) mandate education efforts to address unfair debt collection practices. CE has the potential to make the security clearance investigation process more efficient, effective, and fair, but the ODNI must also take efforts to protect clearance holders from the negative effects of inaccurate credit information.

II. Security Clearance and Reinvestigation Process

The eligibility to access classified national security information, a "security clearance," is an important component of employment in many federal agencies, including in the intelligence community and Department of Defense (DoD), and has become a valuable benefit of federal employment. According to a 2017 ClearanceJobs survey, the average total compensation for security-cleared professionals it surveyed was $86,902.[12] Individuals with a Top Secret security clearance earned an average of $95,868.[13] "The security clearance process is designed to determine the trustworthiness of an individual prior to granting him or her access to classified national security information."[14]

The history of security clearances is traceable to the executive orders issued by Presidents Harry S. Truman and Dwight D. Eisenhower following the end of World War II.[15] President Truman expanded the military classification system created during World War I to all federal agencies in Executive Order 10,290.[16] He also created standards guiding the investigation of employees entering the federal workforce to ensure their "complete and unswerving loyalty" to the U.S., protect "against infiltration of disloyal persons," and give employees "equal protection from

unfounded accusations of disloyalty."[17] This "Loyalty Program," created under the shadow of the Cold War and tensions with Soviet Russia, "has been criticized as a weapon of hysteria attacking law-abiding citizens," but President Truman defended it as a necessary measure to preserve national security.[18] Successive presidents have issued executive orders delegating the classification of sensitive national security information and materials to the heads of agencies.[19] President Eisenhower's Executive Order 10,450 expanded President Truman's order and created many of the factors for consideration that eventually became the 13 adjudicative guidelines used in the present security clearance process.[20]

"An individual who is performing work for the federal government—whether that individual is a direct government employee or a private contractor—may be eligible to obtain a security clearance if his or her work requires access to classified materials."[21] As of October 1, 2017, 4,030,625 individuals were eligible for access to classified information.[22] Generally, only U.S. citizens are eligible to obtain a clearance, but Executive Order 12,968 permits limited access to non-U.S. citizens for certain compelling reasons.[23] The security clearance process is separate from the decision whether an individual is suitable for employment, but a "suitability check" involves "many of the same investigative elements as a security clearance investigation."[24] Even if an individual receives a security clearance, they still cannot access classified information unless they have a "need-to-know" the information.[25] A need-to-know is a determination that the individual needs access to "specific classified information in order to perform or assist in a lawful and authorized government function."[26] The cleared individual also needs to sign a nondisclosure agreement before gaining access to the information.[27]

A. Security Clearance Investigation and Adjudication Process

A security clearance is a formal determination granted by a federal agency or department that a federal employee or government contractor is eligible to access classified national security information.[28] There are three levels of security clearances, "Confidential," "Secret," and "Top Secret."[29] Each level corresponds with the classification level of the information the individual may require access to upon being cleared.[30] Information cannot be classified unless its "unauthorized disclosure could reasonably be expected to cause identifiable or describable damage to the national security …."[31] The classification level of information is based on the level of damage that the information could cause to the national security if improperly disclosed: Confidential information could "cause damage," Secret information could cause "serious damage," and Top Secret information could cause "exceptionally grave damage."[32] Before information can be classified, the federal official classifying the information must be properly delegated by an

official classification authority and must be able to identify or describe the damage that unauthorized disclosure of the information "reasonably could be expected to cause."[33] In addition to these levels, there are two additional categories of information traditionally associated with the Top Secret level, Sensitive Compartmented Information (SCI) and Special Access Programs (SAPs).[34] SCI is a subset of classified information "concerning or derived from intelligence sources, methods or analytical processes that is required to be protected within formal access control systems established by the [Director of National Intelligence (DNI)]."[35] SAPs are programs "designed to control access, distribution, and protection of particularly sensitive information."[36] These two programs require special investigative requirements and procedures.[37] The eligibility standards for these programs are also "higher than for other information classified at the same level, which further restricts the number of individuals that are eligible for access."[38]

In general, the process of obtaining a security clearance traditionally involved four steps: pre-investigation, investigation, adjudication, and reinvestigation.[39] However, Trusted Workforce 2.0 transformed and has essentially replaced the reinvestigation step.[40] During the first step of the clearance process, the pre-investigation phase, the agency makes a determination whether the position that the federal employee or government contractor is applying for or occupies requires access to classified information for the completion of his or her duties.[41] If the position requires access to classified information and the individual does not already have an in scope security clearance, then the employee or contractor will submit clearance application material using the Standard Form 86 (SF 86).[42] Although similar, the SF 85 and SF 85P are used for public trust or non-sensitive positions that do not require access to Secret or Top Secret information and requires a lesser amount of information.[43] Completing the SF 86 is voluntary; however, failing to complete it will likely prevent an individual from gaining eligibility to access classified information and may result in the individual being unable to fulfill the position.[44] Most individuals use the web-based, automated Electronic Questionnaires for Investigations Processing (e-QIP) system to electronically complete and submit the SF 86.[45] The online e-QIP system contains any answers the applicant has previously entered into the system in previous applications, which allows individuals to save time when completing the form for reinvestigations and allows investigators to compare current responses to previous forms submitted by the individual.[46] On September 29, 2019, the National Background Investigations Bureau (NBIB) was realigned from the U.S. Office of Personnel Management (OPM) to the DoD's newly created Defense Counterintelligence and Security Agency (DCSA), but the process for completing the SF 86 has largely remained the same.[47] The individual completing the SF 86 provides information about: his or her citizenship status, family and relatives, personal residences, education history, employment history,

foreign contacts and activities, psychological and emotional health, criminal record, illegal use of drugs and drug activity, previous clearance investigations, financial record, and other information relevant to determining whether the individual is "reliable, trustworthy, of good conduct and character, and loyal to the U.S."[48] In addition to the questionnaire, individuals must provide personal references and authorizations that allow an investigator to access information about the individual, including publicly available social media information, medical information, and consumer credit reports.[49] The applicant certifies the accuracy of this information and submits the information through e-QIP.[50] Any information provided on the form cannot be used in a criminal proceeding against the individual, but "knowingly falsifying or concealing a material fact is a felony."[51]

The second step in the clearance process is the investigation. The information provided by the applicant is sent to the agency sponsoring the individual through the clearance process and the assigned investigative agency begins the personnel security investigation. The investigative agency assigned to complete the investigation depends on the agency sponsoring the individual. The DCSA conducts the majority of investigations across the federal government, but other agencies like the Federal Bureau of Investigation (FBI) have authority to conduct investigations of certain contractor positions.[52] The NBIB "conducts some of the investigative work itself, and contracts out the rest to private firms.[53] The Central Intelligence Agency (CIA) has the authority to conduct its own background investigations and also conducts investigations for the ODNI and other federal agencies.[54] The scope, content, and length of time for an investigation depends on the level of clearance and the agency performing the investigation.[55] The ODNI has set investigation requirements for each access level.[56] For example, a Single Scope Background Investigation (SSBI), a part of every Top Secret clearance investigation, includes interviews with the subject of the investigation, classmates, supervisors and coworkers, former spouses, neighbors, and character references.[57] In addition, it includes records checks of citizenship records, educational institutions, military records, credit reports, criminal history, federal records, and public records (e.g., civil and criminal court actions).[58]

For some sensitive positions, an individual may have to undergo a polygraph examination.[59] There are three different types of polygraph examinations: (1) Counterintelligence Scope Polygraph (CSP) examination, (2) Expanded Scope Polygraph (ESP) examination, and (3) Specific Issue Polygraph (SIP) examination.[60] A CSP examination covers the topics of "espionage, sabotage, terrorism, unauthorized disclosure, or removal of classified information (including to the media), unauthorized or unreported foreign contacts, and deliberate damage to or malicious misuse" of government systems.[61] An ESP examination builds

upon a CSP examination, but also explores the areas of "criminal conduct, drug involvement, and falsification of security questionnaires and forms[,]" among other topics.[62] SIP examinations are only used to resolve specific concerns or to aid in counterintelligence investigations.[63]

The third step of the clearance process is adjudication. Once the background investigation is complete, the sponsoring agency receives the results and makes a determination whether to grant the individual a security clearance.[64] This process is "an examination of a sufficient period of a person's life to make an affirmative determination that the person is eligible for a security clearance."[65] The process uses a "whole person concept" that considers all "reliable information about the person, past and present, favorable and unfavorable."[66] The "final determination remains the responsibly of the specific department or agency," and "any doubt whether to grant an individual access to classified information is clearly consistent with national security will be resolved in favor of the national security."[67] This "clearly consistent with the interests of national security" standard is a lower standard than the traditional preponderance of the evidence standard because this standard "indicates that security-clearance determinations should err, if they must, on the side of denials."[68] The decision whether to grant or continue to grant an individual eligibility is based on consideration of the following thirteen guidelines:

(1) Guideline A: Allegiance to the United States.
(2) Guideline B: Foreign influence.
(3) Guideline C: Foreign preference.
(4) Guideline D: Sexual behavior.
(5) Guideline E: Personal conduct.
(6) Guideline F: Financial considerations.
(7) Guideline G: Alcohol consumption.
(8) Guideline H: Drug involvement.
(9) Guideline I: Emotional, mental, and personality disorders.
(10) Guideline J: Criminal conduct.
(11) Guideline K: Security violations.
(12) Guideline L: Outside activities.
(13) Guideline M: Misuse of Information Technology Systems.[69]

Each of these guidelines represent a potential concern regarding the individual under consideration's allegiance, judgment, discretion, susceptibility to undue influence of coercion, exploitation or duress, or "reliability, trustworthiness, and ability to protect classified information."[70] Adverse information concerning a single criterion is not always sufficient to result in an unfavorable determination.[71] A potential security concern can be mitigated if the individual reported the

information, responded to questions truthfully and completely, sought assistance and followed professional guidance, or has resolved or appears likely to resolve the concern.[72] However, an individual may be disqualified if the "available information reflects a recent or recurring pattern of questionable judgment, irresponsibility, or emotionally unstable behavior."[73]

Guideline F, Financial considerations, is relevant when considering the impact of consumer credit information on the security clearance process. The specific concern under this guideline is that a "Failure to live within one's means, satisfy debts, and meet financial obligations may indicate poor self-control, lack of judgment, or unwillingness to abide by rules and regulations."[74] An individual can mitigate concerns raised under this guideline by showing "the conditions that resulted in the financial problem were largely beyond the person's control …" (e.g., clear victimization by predatory lending practices or identity theft) "… and the individual acted responsibly under the circumstances."[75] In addition, the individual can also mitigate concerns by showing the individual "is adhering to a good-faith effort to repay overdue creditors or otherwise resolve debts" or "has a reasonable basis to dispute the legitimacy of the past-due debt … and provides documented proof to substantiate the basis of the dispute or provides evidence of actions to resolve the issue."[76] Financial considerations have remained the reason for the majority of denials[77] In 2017, the Defense Office of Hearings and Appeals (DOHA) heard 1,844 initial clearance denial appeals for DoD contractors and 1,497 of those denials involved financial considerations.[78]

If the individual going through the adjudication process fails to meet the full adjudicative or investigation standards, the agency can still grant initial or continued eligibility for access to classified information under limited circumstances.[79] These "exceptions" are an explicit adjudicative decision and authorized by the ODNI if approved by the proper authority.[80] Specifically, the agency can grant a "waiver" "when the benefit of initial or continued eligibility clearly outweighs any security concerns."[81] A waiver may include a "condition," or additional security measures to mitigate the concern. Conditions may include "additional security monitoring, access restrictions, submissions of periodic financial statements, or attendance at counseling sessions."[82] An approval authority can also grant a "deviation" if there is a significant gap (six months or longer) in the coverage or scope of the investigation "or the lack of one or more relevant investigative scope components (e.g., employment checks, financial review, or a subject interview) in its entirety."[83] Once an authorized adjudicator has approved an individual for a security clearance or granted an exception, they are eligible to access classified information.

If an agency denies or revokes an individual's clearance, they have an opportunity to appeal the decision based on each agency's procedures in accordance with the guidelines established in Executive Order 12,968.[84] Executive Order 12,968 gives individuals the right to a "comprehensive and detailed written explanation of the basis" for the denial and the evidence upon which the decision is based, including the entire case file, but only as much "as much as the national security interests" of the U.S. and other applicable laws permit.[85] In addition, the individual has the right to be "represented by counsel or other representative at their own expense;" "a reasonable opportunity to reply;" a "personal appearance with the opportunity to present relevant documents, material, and information;" "written notice of and reasons for the results of the review[;] the identity of the deciding authority[;] and written notice of the right to appeal."[86] Any appeal must be to a "high level panel, appointed by the agency head" and "shall be comprised of at least three members, two of whom shall be selected from outside the security field."[87]

Despite these existence of these procedural rights, an agency head has the *conclusive* right to deny an individual the right to any of these procedures if the "head of an agency or principal deputy personally certifies that a procedure … cannot be made available in a particular case without damaging the security interests of the United States by revealing classified information."[88] In addition, an agency head can exercise appeal authority based on recommendations from an appeals panel and his or her decision is final.[89] Denials and revocations make up a small percentage of all security clearance adjudications, but some agencies may discontinue security processing all together if an investigation uncovers automatic disqualifiers discovered when an individual is evaluated to determine their suitability for employment before the individual even enters the security clearance process.[90] In fiscal year 2017, only three of the ten agencies that make up the intelligence community had a denial rate over 4.6 percent, while the rest of the agencies had a denial rate under 2.6 percent.[91] No agency had a revocation rate over 2.3 percent and the majority had a revocation rate under one percent.[92] In fiscal year 2017, 597,423 security clearances were approved.[93]

The fourth step of the clearance process was reinvestigation, but Trusted Workforce 2.0 transformed and is intended to largely replace the reinvestigation step.[94] Clearance holders were required to submit to periodic reinvestigations to ensure their access to classified information is still in the interests of national security by updating a previously completed background investigation.[95] The length of time that a security clearance remained valid depended on the level of clearance and backlogs did result in agencies having to extend some timelines.[96] However, the agency could also reinvestigate an individual "if, at any time, there [was] reason to believe that they may no longer meet the standards for access."[97]

Reinvestigations were expected to be "conducted with the same priority and care as initial investigations" and they followed the same adjudicative guidelines and investigative standards as initial investigations.[98]

B. Judicial Non-Intervention

Although the outcome of a security clearance determination can be appealed administratively, courts have generally declined to review the merits of a security clearance denial beyond ensuring that the agency followed its own procedures.[99] In the seminal case *Department of the Navy v. Egan*, the Supreme Court found that "courts traditionally have been reluctant to intrude upon the authority of the Executive in military and national security affairs" unless "Congress specifically has provided otherwise."[100] In *Egan*, the respondent, a new hire at the Trident Naval Refit Facility in Bremerton, Washington, was denied a security clearance, a requirement for him to be able to board any submarine and perform his duties.[101] After conducting an investigation, the Navy discovered he had past convictions for assault and for being a felon in possession of a gun. In addition, he had failed to disclose two earlier convictions for carrying a loaded firearm and admitted "he had had drinking problems in the past and had served the final days of a sentence in an alcohol rehabilitation program.[102] He had the opportunity to respond to the proposed denial and the Navy's Personnel Security Appeals Board affirmed the denial of his clearance. Mr. Egan sought review of the denial by the U.S. Merit Systems Protection Board (MPSB), "an independent, executive branch agency that works to protect current, former, and prospective federal employees against inappropriate employment-related actions …."[103]

The government's argument before the Board and subsequent appeals was that "the [MSPB]'s review power was limited to determining whether the required removal procedures had been followed and whether a security clearance was a condition" of his employment."[104] The U.S. Court of Appeals for the Federal Circuit reversed a full Board decision holding that the Board did not have the authority to review the merits of a clearance determination underlying a removal. Upon appeal, the Supreme Court held that the President, as "Commander in Chief" under Article II, § 2, of the U.S. Constitution, has the authority "to classify and control access to information beading on national security and to determine whether an individual is sufficiently trustworthy to have access to such information"[105] This authority "flows primarily from this constitutional investment of power in the President and exists quite apart from any explicit congressional grant."[106] Since a security clearance "does not equate with passing judgment," but is an attempt to predict "possible future behavior and to assess whether, under compulsion or for other reasons, [an individual] might compromise sensitive information,"[107] the

"grant or denial of security clearances … is an inexact science at best."[108] Since a security clearance decision involves "predictive judgment" "the protection of classified information must be committed to the broad discretion of the agency responsible"[109] and "it is not reasonably possible for an outside nonexpert body," like a court, "to review the substance of such a judgment."[110] Subsequent to *Egan* courts have embraced this reasoning and generally given absolute deference to the agency making the security clearance decision.[111]

Some critics like Louis Fisher, a specialist in constitutional law, argue the holding in *Egan* has been too broadly construed.[112] Specifically, he argues the majority in *Egan* did not find the President has "plenary or unchecked power over classified information."[113] Rather, he argues the "Resolution of disputes over classified information depends on judgment by both of the elected branches … [and] judicial deference to executive judgments does not require congressional deference."[114] However, several circuits have held that courts have neither the authority nor expertise to review security clearance decisions.[115]

Despite the general presumption against judicial review, the Supreme Court opened the door slightly to some procedural constitutional due process claims in *Webster v. Doe*, which also was decided in 1988.[116] *Webster* involved the removal of a CIA employee based on his sexuality.[117] The court declined to preclude judicial review of constitutional claims unless Congress explicitly precluded such review.[118] The Court held absent a clear intent by Congress to preclude consideration of "colorable constitutional claims," the district court could review such claims.[119] Despite the possibility of judicial review of security clearance decisions in some cases, courts have still generally declined to review such claims.[120]

Also, the U.S. Court of Appeals for the D.C. Circuit has held *Egan* does not insulate "*all* decisions that might bear upon an employee's eligibility to access classified information" from review under Title VII of the Civil Rights Act of 1964.[121] In *Rattigan v. Holder*, the Court held only "expert, predictive judgment made by 'appropriately trained' personnel is insulated from judicial review."[122] In *Rattigan*, a Federal Bureau of Investigation employee alleged his supervisors improperly decided to report him to security clearance investigators.[123] The Court held that an employee's unlawful retaliation claims were not shielded from review because *Egan*'s bar on judicial review only covers "security clearance-related decisions made by Security Division personnel and does not preclude all review of decisions by other … employees who merely report security concerns."[124] Despite this opening, the *Rattigan* court adopted a "knowingly false standard for security reporting claims under Title VII." Therefore, under this precedent an agency will only be liable for discrimination claims where the individuals reporting

security-related information choose to report information they know to be false. These cases demonstrate that most adjudicative decisions and some investigatory steps in the security clearance process are effectively immune from judicial review in most circumstances.[125]

C. Problems with the Security Clearance Process

In recent history, the personnel security clearance process has struggled with investigation backlogs and ineffective cross-agency reciprocity. In fiscal year 2014, investigations for Secret security clearances took an average of 28 days and Top Secret investigations took an average of 77 days to complete.[126] In 2018, there were "more than 700,000 background investigations pending in the NBIB inventory, the average Secret investigation [took] 132 days, and Top Secret investigations [took] 323 days to complete across all of government—including military personnel, direct government employees, and contractors."[127] Backlogs in the investigation process "have existed since as early as 1986, when DoD had more than 300,000 overdue reinvestigations."[128] In 2000, the Government Accountability Office[129] (GAO) estimated that the "reinvestigations backlog for defense, civilian, and contractor personnel was approximately 505,000, with an additional 480,000, which had not been submitted" from DoD and the military departments.[130] In 2000, the military lacked a department-wide database to even measure the backlog.[131] In 2005, the GAO designated the DoD personnel security clearance program a high-risk area.[132] The government-wide personnel security clearance process was added to the GAO's high-risk list in January 2018 and remained on the high risk list in 2019.[133]

In 2018, pursuant to an executive order signed by President Barack Obama, the ODNI, OPM, Office of Management and Budget (OMB), and the Undersecretary of Defense for Intelligence and Security partnered to create the Security, Suitability, and Credentialing Performance Accountability Council (PAC) to focus on eliminating the background investigation backlog, enhance security clearance reciprocity, and improve the security clearance process.[134] The newly formed DCSA was successfully able to reduce "its background investigation inventory from a high of 735,000 in April 2018 to 248,000 in December 2019. With a steady-state inventory target of 200,000 cases."[135] Also, in December 2019 timeliness for Secret investigations was down to 77 days from a high of 96 days and Top Secret investigations were down to 157 days from a high of 254 days.[136] Although the timeliness of investigations and the backlog are currently improving, backlogs in the clearance process have shown to be a recurrent problem throughout the history of the modern security clearance process.

Cross-agency reciprocity has also historically been an area of concern in the security clearance process.[137] "Reciprocity is the acknowledgment and acceptance of an existing background investigation conducted by an authorized investigative agency […] and the acceptance of an active national security eligibility determination granted by an executive branch agency …."[138] Although investigations and clearance eligibility determinations that meet national personnel security standards are supposed to be transferable and "mutually and reciprocally accepted by all agencies,"[139] agencies have failed to follow guidelines and true reciprocity across agencies has been an elusive policy goal.[140] Government contractors in particular, are often left in limbo when transferring between agencies.[141] Reciprocity delays "result in unnecessary overhead costs for contractors that translate into higher contract rates."[142] A rough calculation of the costs caused by these "administrative inefficiencies result each year in the loss of 1,000 contractor labor-years with a total value of $2 billion in the Intelligence Community alone." "The cost to the federal government as a whole could approach … more than $8 billion."[143] In 2018, the ODNI published Security Executive Agent Directive (SEAD) 7 to create uniform and consistent standards on reciprocity in an effort to address reciprocity issues,[144] but SEAD 7 has been criticized for providing too much room for interpretation by agencies.[145] As a result, "many agencies have security policies and procedures that appear to be inconsistent with national-level policy, adding redundant requirements and time delays to clearance transfer requests for both government employees and contractors."[146] The Intelligence and National Security Alliance found that agencies are reluctant to accept clearance decisions by other agencies for three principal reasons: "(1) Ambiguous or misinterpretations of policy and lack of oversight; (2) Inability to see the details behind other agency adjudicative decisions; and (3) Prioritization of government resources allocated to security processing."[147] A modern case management system may help eliminate gaps in implementing reciprocity across agencies.[148] Ultimately, reciprocity problems come down to issues of "turf and trust."[149] Essentially, a determination by agencies "to exert ownership over the security clearances and access held within agencies that reflects the responsibility people feel for the information entrusted to their care."[150] Reciprocity will likely continue to remain a challenge for the security clearance process when considering the differences in workplace and organizational culture at difference agencies across the federal government.[151]

D. Current Changes to the Security Clearance Process

After the September 11th terrorist attacks, Congress passed the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), which President George W. Bush signed into law in 2004.[152] The IRTPA created the ODNI and called for improvements to the security clearance process.[153] Congress's central goal in

creating the ODNI was to have a single official serve as the head of the intelligence community, act as the President's principal intelligence advisor, and integrate the efforts of all of the elements of the intelligence community.[154] One of the items IRTPA mandated was that the President designate a single "department, agency, or element of the executive branch" to be responsible for security clearances and investigations called the "Security Executive Agent" (hereinafter "SEA").[155] The SEA was required to develop and implement a plan to reduce the length of the security clearance process and evaluate the use of information technology and databases in security clearance investigations.[156] The IRTPA also mandated reciprocity among federal agencies and directed OPM to create a unified, secure database on security clearances.[157]

In 2008 President Bush issued Executive Order 13,467, establishing the ODNI as the SEA.[158] It also created the PAC to implement the security clearance reform effort and hold agencies accountable.[159] President Obama amended Executive Order 13,467 to establish the NBIB within the OPM to "serve as the primary executive branch service provider for background investigations."[160] Section 925 of the National Defense Authorization Act for Fiscal Year 2018 (NDAA FY18) gave the Secretary of Defense the authority to conduct security background investigations for DoD personnel and required the DoD to work with OPM to transition the investigation of such investigations from the NBIB.[161] In response to the NDAA FY18, President Donald Trump decided to implement this legislative mandate by transferring responsibility for conducting all background investigations government-wide from OPM to the DoD.[162] Executive Order 13,869 provided direction for realigning NBIB personnel, resources, and functions to the newly named DCSA.[163]

In 2018, the ODNI, which has the "government-wide responsibility to develop, implement and oversee effective, efficient, and uniform policies and procedures for security clearance … investigations and adjudications" announced a new personnel vetting initiative called "Trusted Workforce 2.0" (hereinafter "TW 2.0").[164] The intent of TW 2.0 is to "fundamentally overhaul the federal personnel vetting process and create a new framework of personnel vetting policies, standards, and procedures."[165] The ODNI divided this initiative into two phases.[166] The first phase was to reduce and eliminate the background investigation inventory, which was discussed above, and the second phase is to "establish a new government-wide approach [to personnel vetting] from the ground up."[167] This new vetting model is designed to "speed up the process, reduce complexity, eliminate repetitive and duplicative checks, and mandate better use of resources."[168] Specifically, the intent is that there will be only one vetting model across the entire government with only three different tiers of background investigation tiers: "Tier 1 for low-risk

public trust vetting; Tier 2 for moderate-risk public trust vetting and Secret clearances; and Tier 3 for high-risk public trust vetting and Top Secret clearances."[169] In addition to streamlining the investigation tiers, TW 2.0 also "delineates [five] vetting scenarios tailored around specific mission needs," rather than the previous "one-size-fits-all approach" where every investigation and reinvestigation is treated the same. The first scenario is "Initial Vetting," which is similar to the current initial investigation process.[170] The second is "Continuous Vetting," which will replace the current periodic investigation process with "automated record checks […], agency specific checks, and certain time or event-driven fieldwork."[171] The automated record checks process in this scenario will use CE capabilities and processes.[172] The third scenario involves "Upgrades," or the move to a higher-level risk position or higher level of security clearance.[173] The fourth scenario, "Transfer of Trust," is designed to address ongoing challenges with reciprocity and improve the mobility of individuals between agencies.[174] The fifth and final scenario, "Re-establishment of Trust," will improve the vetting of individuals who have taken a break from serving in a sensitive position and allow the individual to return more expediently to the workforce.[175]

III. Continuous Evaluation and Consumer Credit Information

CE or "Continuous Vetting"[176] is a concept and set of capabilities that will play a larger role in the security clearance investigation process under TW 2.0. In the security clearance and vetting process, CE involves "reviewing the background of an individual who has been determined to be eligible for access to classified information … at any time during the period of eligibility to determine whether the individual continues to meet the requirements for eligibility"[177] It includes the review of "additional or new checks of commercial databases, Government databases, and other information lawfully available to security officials."[178] CE was originally "intended to fill the gap that exists between periodic reinvestigations, but under the new Continuous Vetting concept, it will now essentially replace much of the periodic reinvestigation process."[179] Brian Dunbar, the Assistant Director of the National Counterintelligence and Security Center, said the transition away from periodic reinvestigations turns the security clearance eligibility process "from a date driven system—where focus was on periodic investigation or initial investigation dates—to a risk based system. The focus will be less on whether or not applicants are 'in scope'—but rather, when they were last enrolled, and what, if any issues, were present at that time."[180] As of March 2020, the DoD has already enrolled nearly 1.4 million of its clearance holders into CE programs under these new processes.[181]

CE involves automated record checks conducted on a more frequent basis than those conducted during periodic investigations, but the types of records checked are the same as those previously checked during the investigation process.[182] According to the ODNI, CE consumer credit checks are similar to employment "soft inquiries" of an individual's credit report like other credit checks conducted for employment purposes in the private sector.[183] Essentially, CE programs alert agencies "to potential red flags on a clearance holder's credit or financial transactions," giving agencies "a near-real-time look at its trusted population."[184] For example, an agency is able to get near-real-time information about an individual's missed credit card payment or default on a student loan.[185] Any relevant information discovered during the course of CE is investigated and adjudicated under the same existing standards that currently exist in the clearance process.[186]

Executive Order 12,968, as amended, tasks the ODNI with the responsibility of establishing the standards for CE and providing oversight over its implementation.[187] Despite the current focus on CE, CE in the security clearance realm is not a new concept. The DoD has piloted aspects of continuous evaluation since at least 2002, including the "technical capability to conduct automated record checks from over 40 government and commercial databases."[188] These "commercial databases" include consumer credit information from consumer reporting agencies.[189] After the September 2013 shooting at the Washington Navy Yard, the DoD issued DoD Instruction 5200.02 which states "all personnel in national security positions shall be subject to [CE]."[190] Consistent with this instruction, the DoD implemented a CE pilot in 2014.[191] A similar pilot is also underway at the Department of State.[192] In 2018, the ODNI issued SEA Directive 6 (SEAD 6), which establishes policy and guidance for CE, but the ODNI has still been criticized by the GAO for failing to "complete plans to fully implement and monitor" CE and its development across agencies.[193]

IV. Consumer Credit Reporting and Debt Collection Practices

A. Credit Reporting Agencies

Consumer credit reports play an increasingly important role in the lives of all U.S. consumers.[194] The majority of decisions "to grant credit—including mortgage loans, auto loans, credit cards, and private student loans—include information contained in credit reports as part of the lending decision."[195] However, credit reports have also found their way into "other spheres of decision-making, including eligibility for rental housing, setting premiums for auto and homeowners insurance in some states, or determining whether to hire an applicant for a job."[196] As discussed above, credit reports will also have an increasingly

important role in CE programs.[197] As the range of decisions that rely on credit reports has increased, so has the importance of ensuring that the credit information contained in these reports is accurate.[198]

The first consumer Credit Reporting Agencies (CRAs) in the U.S. emerged in the late nineteenth century as a way of helping merchant lenders extend credit to local business and individuals.[199] Before the advent of CRAs, merchants only extended a very small amount of credit largely based "on the merchant's direct personal knowledge of the individual borrower's personal character."[200] "Beginning in the 1920s with the introduction of retail installment credit and continuing in to the 1950s with the introduction of revolving credit accounts, credit reporting became increasingly important to both lenders and borrowers.[201] Throughout the 20th century, the CRA industry began to consolidate as computer databases became more technologically advanced and the importance of offering nationwide coverage became more important to credit card issuers and automated underwriting for lenders.[202] Today the three main nation-wide credit bureaus, TransUnion, Experian, and Equifax, receive approximately 1.3 billion updates for over 200 million consumer files each month.[203] These three major CRAs have information on "virtually every adult American citizen and they routinely prepare credit reports about individuals."[204] CRAs prepare consumer reports based on an individual's financial transactions history data.[205] This data may include "historical information about credit repayment, tenant payment, employment, insurance claims, arrests, bankruptcies, and check writing and account management."[206] Firms or companies that use consumer reports also report information to CRAs and become "furnishers" of information to CRAs.[207] A "tradeline" is an account attached to an individual consumer that is reported to a CRA by a furnisher and serves as a record of the payment activity associated with the account.[208] The decision to furnish a tradeline to a CRA is voluntary and furnishers have a variety of different business models and policies covering how they report credit information to CRAs.[209]

In 1970, Congress passed the Fair Credit Reporting Act (FCRA) to regulate CRAs.[210] The passage of the Act was "inspired by allegations of abuse and lack of responsiveness of credit agencies to consumer complaints."[211] Congress passed the FCRA for the express purpose of insuring that CRAs "exercise their grave responsibilities with fairness, responsibility, and a respect for the consumer's right to privacy."[212] The FCRA requires CRAs to provide individuals "access to [the individual's] records, establishes procedures for correcting information, and sets limitations on disclosure" of credit reports.[213] A CRA is defined as "any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer

credit information or other information on consumers for the purpose of furnishing consumer reports to third parties."[214]

In 2003 Congress amended the FCRA by passing the Fair and Accurate Credit Transaction Act (FACTA). The impetus of FACTA was the pending expiration of the provisions that preempted state laws affecting CRAs under the FCRA.[215] In addition, consumer and privacy groups had continued to express concerns that the FCRA was not addressing many of the long-standing problems with CRAs, namely "inaccuracy, faulty reinvestigations, reinsertion [of previously deleted material], non-responsiveness, and lax security."[216] In addition, the crime of identity theft had become the "nation's 'fastest growing crime.'[217] The biggest harm from identity theft was the privacy of credit reports."[218] As a result, FACTA added some measures to the FCRA to help address identity theft. Specifically, FACTA allows an individual to report potential fraud to one CRA and the CRA is then required to notify the other major CRAs.[219] If an individual identifies information on their credit report that is the result of alleged identity theft the CRA must block the reporting of that information.[220] In addition, it requires CRAs to provide a free copy of a consumer's credit report once per year when requested by the consumer.[221]

CRAs are required to "follow reasonable procedures to assure maximum possible accuracy of the information concerning the individual about whom the report relates."[222] If an individual discovers an error in his or her credit report and notifies the CRA of the error, the agency is required to conduct a "reinvestigation" of the error for free and it must "record the current status of the disputed information or delete the item from the file."[223] The CRA is required to provide written notice of the results of the reinvestigation within five business days after they complete the reinvestigation and delete any inaccurate, incomplete, or unverifiable information.[224] An individual is permitted to file a dispute with the CRA if the reinvestigation does not resolve the dispute and the CRA is required to note that the information is disputed when providing the credit report to third parties under most circumstances.[225]

Since CRAs are only required to provide "reasonable procedures to assure maximum possibly accuracy," a CRA is not automatically civilly liable for providing inaccurate credit information. In many cases, courts have found that CRAs are not liable, as a matter of law, for reporting inaccurate information "unless there was prior notice from the consumer that the information might be inaccurate."[226] Some legal commentators have criticized the FCRA for being too deferential to CRA interests and questioned whether negligence is the best fault standard for liability.[227] CRAs and those that furnish data to CRAs also have qualified immunity

from state tort laws, like defamation, under the FCRA and an individual can only file state tort actions when a CRA or furnisher "acted with malice or willful intent to injure."[228]

Despite the passage of FCRA and subsequent amendments, two main issues have dogged the consumer credit report industry: identity theft and inaccurate information. In 2016, an estimated 26 million people in the U.S., about 10 percent of all U.S. residents over the age of 16, had been the victim of identity theft during the previous year.[229] The U.S. Department of Justice estimates the total losses across all incidents of identity theft was $17.6 billion in 2016.[230] Nearly one in five people (49.7 million people) in the U.S. have experienced identity theft in their lifetime.[231] Although the majority of victims are able to resolve financial and credit issues associated with identity theft in an average of about four hours total, victims of multiple types of identity theft spend an average of 22 hours resolving associated problems.[232] When identity thieves generate fraudulent debts in the names of individuals, those delinquencies are reported to the CRAs and they appear on an their credit reports. As a result, "A significant amount of identity theft involves the consumer reporting system."[233] Daniel Solove argues the way credit is issued in the U.S. is the cause of the identity theft problem.[234] Specifically, he points to the bad practice of companies "using SSNs, mother's maiden names, and addresses for access to account information." In addition, this problem is exacerbated by the fact many creditors "give out credit and establish new accounts if the applicant supplies a name, SSN, and address."[235] Even as financial institutions improve their security measures, Lynn LoPucki has pointed out, "The problem is not that thieves have access to personal information, but that creditors and [CRAs] often lack both the means and incentives to correctly identify the persons who seek credit from them or on whom they report."[236]

Many of the critiques of CRAs and consumer credit reporting in general revolve around the presence of inaccurate, incomplete, or misleading information in credit reports. In 2016, the Consumer Financial Protection Bureau (CFPB) reported the three main CRAs were the three most-complained-about companies in the U.S.[237] In an oft quoted 2015 U.S. Federal Trade Commission (FTC) study on credit reporting errors, 26 percent of study participants had "potentially material errors" on at least one of their credit reports[238] In fact, "1 in 20 consumers have errors so serious that they would be denied credit or need to pay more for it."[239] Some of the inaccuracies that pervade the credit reporting system include: (1) mixed files, where information belonging to one consumer is reported in another consumer's report; (2) furnished errors, which include furnishers incorrectly recording payment history, attributing a debt to the wrong consumer, or including debt that is older than the seven years permitted under the FCRA;

(3) identity theft; and (4) ignored judgments and legal settlements, where CRAs retain information even after judgments or settlements declare that a consumer does not owe a debt.[240] Unfortunately, in the credit reporting system, "Speed and volume are favored over accuracy. Large-scale inaccuracies are tolerated. The costs of correcting data outweigh benefits—for the credit bureaus, though, not the consumers."[241] CRAs "have little economic incentive to conduct proper disputes or improve their investigations" because consumers are not their primary customers.[242] Problems with inaccuracies have spawned lawsuits, state investigations, and proposed federal regulations.[243] Under a settlement reached in 2015 between the three main CRAs and the Attorney General of New York State, the CRAs agreed to "overhaul their methods of fixing errors."[244] In light of these problems, the National Consumer Law Center has suggested reforms to the credit reporting system that include, among other proposals, requiring stricter matching criteria when matching information to consumers and requiring CRAs to "devote sufficient resources and conduct independent analyses in disputes."[245]

B. Fair Debt Collection Practices

Although credit reporting is a frequent source of consumer complaints handled by the CFPB, they are only the second most frequent source of complaints behind the number one driver of complaints: debt collection.[246] The debt-collection industry has grown over the past four decades as the availability of consumer credit has expanded and the debt collection industry has evolved its methods.[247] In 1977 Congress passed the Fair Debt Collection Practices Act (FDCPA) to protect consumers from unfair, deceptive, and abusive debt collection practices.[248] The FDCPA prohibits particular collection practices, such as harassment and the use of false or misleading representations.[249] The Act authorizes private individuals to sue for damages against violators in addition to certain federal agencies.[250] Under the statute, a "debt collector" includes "any person … in any business the principal purpose of which is the collection of debts, or who regularly collects or attempts to collect … debts owed or due or asserted to be owed or due another."[251] In addition to the FDCPA, many states have enacted laws or issued regulations that regulate the activities of debt collectors in comparable ways to the FDCPA.[252]

In 2019 alone, the CFPB and the FTC, which share enforcement responsibility of the FDCPA, engaged in 30 public enforcement actions against debt collectors and secured almost $50 million in consumer redress and $35.9 million in civil penalties and judgments.[253] Even if many debt collectors comply with consumer protection laws, some "harass and threaten consumers, demand larger payments than the law allows, refuse to verify disputed debts, and disclose debts to consumer's employers, co-workers, family, members, and friends."[254] In 2019,

the CFPB received approximately 75,200 debt collection complaints.[255] The most common debt collection complaint was about attempts to collect a debt that the consumer reported was not owed.[256] This problem could be correlated to the rise of the "debt-buying," where debt is sold by "creditors or other debt owners to buyers that then attempt to collect the debt or sell it to other buyers."[257] In a 2009 study, the FTC "expressed concern that debt collectors, including debt buyers, may have insufficient or inaccurate information when they collect on debts, which may result in collectors seeking to recover from the wrong consumer or recover the wrong amount."[258] In addition, in 2020 the CFPB also found the "proportion of complaints about debts resulting from identity theft has been increasing for several years."[259] "These complaints often involve consumers reporting to credit bureaus that they have negative tradelines on their credit reports due to identity theft."[260] In some other cases, consumers reported "companies impersonated an attorney or a law enforcement or government official" or" indicated the consumer committed a crime by not paying a debt."[261] Advocacy groups like Consumer Reports complain, "Far too many consumers continue to report that debt collectors hound them about [debt] they have already paid off or never owed in the first place."[262] In many cases, "Debt collectors often lack proof that the debt even existed let alone that the person they are targeting is responsible for it."[263]

Under the FDCPA, a consumer contacted by a debt collector has several rights. The consumer has the right to a written notice that includes the amount of the debt, the name of the creditor, dispute rights, and the right to request information about the original creditor, if different than the current creditor.[264] A consumer also has the right to request in writing that a debt collector cease communications with the consumer.[265] Although this will not extinguish an otherwise valid debt, it will prevent the debt collector from contacting the consumer regarding the debt except under limited exceptions.[266] Debt collectors are barred from "using obscene or profane language, threatening violence, calling consumers repeatedly or at unreasonable hours, misrepresenting a consumer's legal rights, disclosing a consumer's personal affairs to third parties, and obtaining information about a consumer through false pretenses."[267] Each state has its own statute of limitations on debt collection.[268] It is considered a violation of the FDCPA to file suit to collect a debt that is "time-barred" (older than the statute of limitations). However, in some states a debt collector can collect time-barred debts as long as the debt collector does not threaten to pursue litigation.[269] In some states, a partial payment on a time-barred debt can renew a creditor's ability to sue.[270] As a result, a consumer can be misled into making a partial repayment and restarting the statute of limitations.[271] Regardless of whether a debt is time-barred, a debt collector can report debt to CRAs and it could appear on an individual's credit report as long as the debt is less than seven years old.[272] Despite the protections afforded to

consumers under the FDCPA and state law, the debt collection industry continues to face consumer protection concerns especially for consumers who may not be aware of their legal rights.

V. Protecting Clearance Holders From Erroneous Consumer Credit Information, Bias, and Unfair Practices

The incorporation of consumer credit information into the CE process risks creating unfair situations for a workforce that relies upon security clearances to maintain employment. There are several ways the ODNI can protect current clearance holders from the effects of erroneous or misleading consumer credit information: (1) mandate an effective, centralized investigation database that prevents the reflagging of previously adjudicated issues in credit records; (2) ensure appropriate oversight and burden sharing among agencies, CRAs, and clearance holders; (3) require the reporting and analysis of automated records check systems to identify potential bias or disparate impacts on protected classes and minority groups; and (4) mandate education efforts to address unfair debt collection practices.

A. Centralized Investigation Database

A centralized investigation database that prevents the reflagging of previously adjudicated issues in credit and financial records is necessary to prevent clearance holders from being flagged for the same potential derogatory data coming from different commercial databases. According to the ODNI, the CE program currently reviews "information that is already reviewed during [current] background or periodic investigations," but the automated nature of these checks changes the dynamic of the investigative process.[273] Under the previous reinvestigation process, a clearance holder may have had the opportunity to review their credit reports from all of the major CRAs before submitting their SF 86, or during the investigation, to ensure the information on their credit reports was accurate. During this process, the clearance holder had the ability to address those entries, at least initially, with the CRA, the furnisher of the information, or their agency's security professionals; build supporting documentation; or find ways to pay off or negotiate with a debt collector to resolve negative information. This meant that the security clearance holder may have had the ability to address their records and may have had time to correct mistakes or at least begin to address an inaccuracy. The CE program eliminates this valuable lead time and control. Although the ODNI has stated "If inaccurate information is identified during [CE] records checks, subsequent records corrections will be handled in the same manner as it is today by the personnel security investigative processes,"[274] the frequency of these checks and the potential that multiple commercial databases may

report information at different intervals means that a clearance holder may need to address the same or similar negative information with investigative personnel multiple times.

Without a centralized investigation system, the burden placed on clearance holders to address erroneous credit information could unfairly affect clearance holders. Interagency reciprocity, one of the main challenges of clearance holders attempting to move between federal agencies, may only become more difficult to implement with the elimination of periodic reinvestigations.[275] Clearance holders may be subject to reinvestigation for issues they have already successfully mitigated, explained, or identified as erroneous when working for another agency. A centralized investigative and reporting database would allow an agency to review how previous adverse information was addressed by investigatory personnel, security professionals, and the clearance holder themselves.[276] If a clearance holder is a victim of identity theft, multiple erroneous pieces of financial information could appear on a person's credit report at a variety of intervals. Without a centralized investigation system, the clearance holder may be forced to address each of these erroneous entries individually on a frequent basis, rather than being able to show she was a victim of identity theft, she took steps to "freeze" her credit reports, she reported the theft of their identity to law enforcement, and she had outlined all of the credit entries that were erroneous as they could do under the previous security clearance investigation process. A security manager or security professional assigned to a clearance holder will likely know an individual has been a victim of identity theft and can work with him or her to address individual pieces of erroneous credit information in a way that causes a minimal disruption to their work. If this information is not centrally recorded and accessible then a clearance holder will need to readdress the same concerns if they move to a different agency, transfer to a new position in an agency, or a new security manager is assigned to the employee. Under the previous system, a clearance holder at least had the opportunity to address erroneous credit information that exists in consumer reporting databases when they are periodically investigated so a clearance holder can prepare and update any previous information they have provided to investigators, but continuous evaluation changes that timeline and could result in a clearance holder being unfairly burdened responding to inquiries from their security manager or other investigative personnel. In addition, if a government civilian employee's clearance is suspended or revoked because of erroneous credit information, the employee could be immediately suspended without pay while the issue is adjudicated.[277] A contractor could also find themselves terminated if their clearance is suspended. Since the contractor no longer has an affiliation with the agency, the agency may determine it no longer has jurisdiction to adjudicate the suspension or revocation of the clearance.

A successful centralized investigation database will need to include cross-agency accessibility and the ability for clearance holders to view and submit their own information regarding identify theft, fraud, or other consumer credit errors. The DoD's current CE program pulls in some data from the ODNI's CE program, which the ODNI operates as a service to a variety of agencies, but the DoD still has its own system.[278] Reciprocity, "one of the most vexatious aspects of the system of granting security clearances," is an "elusive policy goal that has been pursued since the Clinton Administration."[279] The underlying issue with complete reciprocity among agencies is a "lack or trust based on fear."[280] Security Executive Agent Directive 7 (SEAD 7) is the latest attempt to resolve this problem.[281] In SEAD 7, the ODNI mandates agencies accept background investigations and national security eligibility adjudications completed by an authorized agency with certain limited exceptions.[282] SEAD 7 does not mandate a centralized database, but instead requires agencies to conduct a review of the databases that currently contain records of prior national security eligibility adjudications.[283] The intelligence community uses Scattered Castles, the DoD used the Joint Personnel Adjudication System (JPAS) (which has now been replaced by the Defense Information System for Security (DISS)), and OPM currently uses the Central Verification System (CVS) to record and maintain clearance information.[284] Although JPAS and CVS had a data bridge for clearance reciprocity purposes[285] and the ODNI has directed the intelligence community to collaborate with the DoD and OPM to ensure security information in Scattered Castles is correlated with OPM's CVS database, the databases largely operate independently.[286] "Greater information-sharing regarding personnel clearances among and between government agencies assists transparency and can help security officers trust other agencies' clearance decisions."[287] "At the core of many reciprocity delays is the inability of federal agencies to see the rationale for the clearance eligibility decisions made by other agencies."[288] "[G]overnment agencies often cannot see the details behind the investigative and adjudicative records of other agencies, which often makes them reluctant to grant reciprocal access."[289] The enrollment of clearance holders into CE can also hinder them if they try to change employers and the new agency does not see a periodic reinvestigation at the mandated time in their records even though enrollment in CE removed the requirement for a reinvestigation.[290] A centralized adjudication database with cross-agency accessibility could help solve reciprocity problems and build trust among agencies. DCSA has continued to develop the National Background Investigation Services (NBIS), which is intended to serve as "the federal government's one-stop-shop IT system for end-to-end personnel vetting—from initiation and application to background investigation, adjudication and continuous vetting."[291] If NBIS CE capabilities help protect clearance holders from inaccurate or previously flagged consumer credit information and all agencies are committed to its future development, NBIS

could aid in cross-agency transparency and may help security officers trust other agencies' clearance decisions.

There are risks to creating a centralized government system that includes sensitive personal and financial information. Any large government database, especially one with the personal information of clearance holders, is a target for hackers and presents a possible risk to national security. In 2015, the public learned of massive data breaches at the OPM. "In what appears to be a coordinated campaign to collect information on government employees, attackers exfiltrated personnel files of 4.2 million former and current government employees and security clearance background investigation information on 21.5 million individuals."[292] "Officials have privately attributed the breach to the Chinese government."[293] The then-Chief Information Officer at OPM, Donna Seymour, admitted during a hearing before the House Oversight and Reform Committee in June of 2015 that the data compromised in the data breach included information from SF 86s and clearance adjudication information.[294] Former U.S. National Security Agency Senior Counsel Joe Brenner called this information "crown jewels material … a gold mine for a foreign intelligence service."[295] Representative Jason Chaffetz, the then-chairman of the House Government Reform Committee placed the blame for the breach squarely on OPM leaders.[296] "By ignoring repeated warnings of system vulnerability, failing to adopt basic cybersecurity best practices and wasting millions of dollars maintaining outdated technology, OPM leaders left the agency's valuable data vulnerable to attack."[297] In his opinion, "The resulting breach was entirely predictable and its risk well known." The attack was the result of negligence, inadequate cybersecurity measures, mismanagement of IT budgets over decades, poor data management and incompetent leadership."[298] The consequences of this breach are still unfolding. In September 2015, the Washington Post reported the CIA pulled officers from the U.S. Embassy in Beijing, China, as a "precautionary measure" in the wake of the breach.[299] The reported reason for the action was, 'Because the OPM records contained the background checks of State Department employees, officials privately said the Chinese could have compared those records with the list of embassy personnel. Anybody not on that list could be a CIA officer."[300] Even four years after the breach, the data is being used in financial crimes here in the U.S.[301] In 2018 in Virginia, two criminals used information from the breach to take out fake loans using stolen identities.[302] Even with the substantial risks associated with aggregating and centralizing this information, a centralized database with appropriate cybersecurity measures is the best way to help mitigate the challenges that CE will bring to the clearance process. There is no way to avoid using databases and a cross-agency centralized system will allow a consolidation of expertise, funding, and focus. In 2016, the Majority Staff of the House Committee on Government Oversight and Reform,

made it clear that prioritizing and securing critical systems could have mitigated the damage from the breach and the federal government needs to improve its recruitment, training, and retention of cyber security specialists.[303] A centralized system will help establish clear sources of funding and decision-making processes for IT security.[304]

The ability for clearance holders to report their own information regarding identify theft, fraud, or other consumer credit errors in the system could also prevent unnecessary investigations and resolve repeat alerts. Although the CE process permits a clearance holder to provide information to an assigned security professional to mitigate or explain adverse information, a formal way to include this information in a central system would allow subsequent security professionals or other agencies to consider potentially adverse information in the full context when making decisions about continued eligibility. The FCRA already includes a similar requirement in the context of consumer credit reports.[305] Under the FCRA, a CRA is required to complete a "reinvestigation" to determine whether disputed information on a credit report is inaccurate.[306] Even if the reinvestigation does not resolve the dispute, the CRA is required to allow the consumer to submit a "brief statement setting forth the nature of the dispute."[307] The CRA is permitted to limit these statements to not more than 100 words if it assists the customer write a clear summary of the dispute.[308] Most importantly, unless the dispute is "frivolous or irrelevant," the CRA is required to include the statement in subsequent consumer reports provided by the CRA.[309] An analogous process could be included in a CE context to allow clearance holders to include a formal dispute of any adverse information in the central database even if the security manager does not initiate an investigation.[310] This would allow any future security manager or investigator to see that the flagged consumer credit information is possibly inaccurate. It could also allow a clearance holder to include information in the record that could help resolve future CE alerts. Including this process would save the time of clearance holders, security professionals, and investigators, but it would also give clearance holders a measure of agency in the CE process. Regardless of its features, a centralized investigation database would go a long way to protecting clearance holders from inaccurate or previously flagged consumer credit information.

B. Appropriate Burden Sharing and Oversight

Given the inaccuracies present in many consumer credit reports, the ODNI needs to establish appropriate guidance and policies governing the use of consumer credit information in CE and ensure appropriate oversight and burden sharing among agencies, CRAs, and clearance holders. As the number of clearance holders enrolled in CE expands, the ODNI should ensure automated systems do not produce

a backlog of unaddressed erroneous credit information. In addition, CRAs should bear some of the burden of ensuring their information is accurate. Although the ODNI has stated automated "alerts" will only be treated as leads, regulations and processes need to further clarify this policy.[311] According to the ODNI,

> Any derogatory identified during CE automated records check will be used for investigative lead purposes only. This information will subsequently be investigated according to existing personnel security processes. No action will be taken based solely on the adverse information identified during the CE process without follow-up and review by the adjudicating agency against established national security adjudicative guidelines.[312]

If the alert identifies inaccurate information, "subsequent records corrections will be handled in the same manner as it is today by the personnel security investigative processes."[313] According to SEAD 6, the ODNI policy governing CE, "investigative agencies shall make reasonably exhaustive efforts to verify that any information collected that is discrepant or potentially disqualifying pertains to the covered individual."[314] In addition, "no unfavorable personnel security actions shall be taken solely on uncorroborated or unverified discrepant information."[315] Despite these stated policies, the DoD's regulations regarding CE state "the ultimate responsibility for maintaining continued national security eligibility rests with the individual."[316]

Treating CE automated records alerts for consumer credit information as leads that agencies have to process according to current personal security procedures rather than dispositive adverse information is the only way to ensure that the contextualized decision-making is left to human discretion.[317] The legacy personnel security investigative process has led to significant backlogs,[318] but it is also important that CE processes do not create new backlogs. Although the ideas incorporated into TW 2.0 and its accompanying changes to the security investigative process are anticipated to help prevent backlogs in the investigation and adjudication process, CE could also result in a backlog of unaddressed and unverified flags generated by CE processes.[319] The federal agencies that have enrolled their workforces in CE have not publicly released information on whether it has improved the efficiency of the process nor how many alerts are regularly processed. As CE record checks proceed autonomously and agencies continue to expand the number of personnel enrolled in the program, security professionals and investigators could become overwhelmed and the benefits of an autonomous system could be mitigated by a backlog of unresolved flags. The ODNI has already made revisions to the "investigative flags" for certain "financial delinquencies and

traffic fine violations," but there is no publicly available information on what those changes were or why they were necessary.[320] If investigators or security professionals become overwhelmed with unresolved investigative flags, it is not unforeseeable that they will shift much of the burden on addressing these alerts with the clearance holder rather than the investigator.[321] Although there is nothing wrong with shifting some of the burden of proving suitability for continued access to the clearance holder, CE is supposed to improve the efficiency of the security clearance process, not unnecessarily extend the reinvestigation process and create a new type of backlog of insufficiently investigated potential adverse information.

Since CE currently relies on commercial databases, government databases, and other information available to security officials,[322] the presence of inaccurate information in consumer credit reports could result in significant numbers of clearance holders having to address erroneous information. If CE is going to continue to use commercial databases, then some of the burden of ensuring the accuracy of those databases needs to be placed on those commercial providers. In the civilian consumer financial data context, courts have held that a CRA is "not liable under the FCRA if it followed 'reasonable procedures to assure maximum possible accuracy,' but nonetheless reported inaccurate information in the consumer's credit report."[323] The FCRA is criticized as being too deferential to industry interests by inadequately protecting "individuals from the consequential and emotional damages caused by misattributed acts."[324] Under the FCRA, courts have generally not found CRAs liable for reporting information that might be inaccurate unless there was prior notice from the consumer that the information might be inaccurate.[325] Ultimately, the real roots of the problem of erroneous data and identity theft is that CRAs "often lack the means and the incentives to correctly identify the persons … on whom they report."[326] Since the government already maintains databases of identification information that clearance holders submit, including biometric data and other personal information, the government, working with CRAs, has much of the information needed to identify erroneous information if properly utilized. However, creating a more sophisticated information system integrating this type of personal information might cause other significant privacy related problems.[327] Also, CE programs could embrace machine learning programs or artificial intelligence to help sort through consumer credit data. Regardless of the method, the government should require greater accuracy from CRAs when they use the consumer credit data CE purposes. Even if agencies are unwilling or unable to integrate data from personnel records and commercial sources, investigators can take steps to ensure inaccurate financial data is properly excluded from consideration before it is considered adverse information. Specifically, agencies can require that commercial sources take active steps to ensure that identified derogatory credit information is accurate, including: (1) requiring furnishers to

ensure personal information connected to a credit line actually matches that of the clearance holder;[328] (2) requiring the furnisher provide proof of the debt or late payment to the CRA for reporting to agencies; and (3) providing real-time credit monitoring services to clearance holders enrolled in CE. These steps would cause increase the cost of clearance programs, but it would encourage agencies to identify the specific types of records that deserve scrutiny and encourage CRAs to verify the accuracy of the information they provide. Providing credit monitoring to clearance holders would result in significant costs to agencies, but it is the only way to ensure clearance holders have real-time, accurate information about what is included on these commercial databases and can take steps to address erroneous information that has the potential to affect their continued eligibility for access. After the OPM breach in 2015, the OPM and DoD entered into an over $133 million contract with a third-party identity monitoring company to provide identity theft protection services for the 21.5 million individuals whose background check information was stolen in the breach.[329] This contract provided "all impacted individuals and their dependent minor children … with credit monitoring, identity monitoring, identity theft insurance, and identity restoration services for a period of three years."[330] However, when comparing the cost of these services to the investigative costs associated with personally investigating each piece of potentially adverse information, it may make more sense to allow clearance holders to play a role in identifying incorrect information since they have a personal interest in removing or correcting inaccurate credit information. Under the law individuals only have the right to request one copy of their credit report for free from each of the major CRAs once a year.[331] If agencies will be accessing this consumer credit information in real-time through active monitoring rather than at periodic intervals, then clearance holders should not have the bear the burden of paying for real-time credit monitoring to protect themselves.

In addition to the steps that commercial agencies can take, agencies or the ODNI can outline the specific investigatory steps that an agency will be required to take to ensure "investigative agencies … make reasonably exhaustive efforts to verify that any information collected that is discrepant or potentially disqualifying pertains to the covered individual."[332] These steps should include requiring the investigator to request and receive underlying proof of the debt or potentially adverse information before asking a clearance holder to address the credit information entry. They should also include requiring an investigator to compare the personal information listed on the credit record to the personal information provided by the clearance holder on their SF 86 or other personnel records. These steps could help eliminate the consideration of credit obtained through fraudulent means and force CRAs to reinvestigate disputes quickly since their customer, the federal government, is requesting this information rather than the consumer. Whether the

some of the burden for ensuring consumer credit information is accurate is placed on investigative personnel or CRAs, appropriate burden sharing and oversight is necessary since consumer credit information is a part of the CE process.

C. Safeguards Against Bias and Discrimination

Federal agencies should also be required to regularly report and analyze their automated records check systems to identify and prevent bias and disparate impacts on protected classes and minority groups, especially if these record check systems use machine learning. DCSA is reportedly "piloting a new clearance evaluation system powered in part by machine learning."[333] This pilot is intended to join data from CE programs and other digital information to identify "micro changes in behavior" to help prevent suicides, data breaches, or other insider threat risks.[334] The attractiveness of using an autonomous system and artificial intelligence (AI) to identify risks before they become threats is obvious, but "pinning individuals' clearance statuses – upon which many rely for their livelihoods, and to work effectively in service of national security – to automated inference-making raises a range of troubling questions."[335] Risk assessment tools similar to those envisioned by DCSA have been shown to be "harsher to certain demographic groups" when used in predictive programs in the criminal justice system and could have similar outcomes if used in CE programs.[336] "AI can help identify and reduce the impact of human biases, but it can also make the problem worse by baking in and deploying biases at scale in sensitive application areas."[337] Although this problem is not new, the sophistication of AI technology has grown considerably as the use of AI has gradually expanded across different sectors.[338] Experts in the field have identified several key challenges to addressing the problem of bias in AI, including: (1) bias built into data, (2) amplification of bias as AI algorithms learn or evolve, and (3) understanding and measuring "fairness."[339]

The first problem is the bias built into the data. The data that are fed into AI algorithms may already have discrimination built in based on the indirect influence of bias.[340] "As the popular computer science maxim explains, "'garbage in, garbage out' meaning biased inputs (source data) will lead to biased or erroneous outputs."[341] Credit providers already use job history, previous salaries, and access to credit to determine creditworthiness even though race and gender have shown to have a negative impact on each of these data points.[342] Data gives AI sustenance that it can use to learn at faster rates than humans; however, if this data has built in biases then AI's objective algorithms will already be tainted by the influence of bias.[343]

The second problem is that biases are amplified as AI algorithms learn and evolve. Even if the data inputted in AI algorithms is free from the influence of bias, these algorithms are not static. Many "learn and change over time" as the system gains experience.[344] "Notably, these changes are not due to human intervention to modify the code, but rather to automatic modifications made by the machine to its own behavior."[345] These algorithms "learn to make decisions independently; in other words, the algorithms learn to make decisions that reach beyond explicitly programmed instructions."[346] "Inaccuracies and biases in data may be amplified" because these "algorithms function autonomously, independently selecting and analyzing variables, adopting processes, and drawing conclusions."[347]

In an analogous context, the historic discriminatory practice of "redlining," where the government-sponsored Home Owner's Loan Corporation outlined areas with large Black populations on red ink on its maps as a warning to mortgage lenders, resulted in overt discrimination with lasting effects.[348] Studies have shown that "in cities with a history of redlining, the redlined areas today generally remain more segregated and more economically disadvantaged."[349] In an AI context, redlining behavior could occur if AI "evolves" to associate certain communities with safer investments or an increased risk of disloyal behavior, but such a process could be hidden from an expert or program administrator and they could be unaware they are engaging in an unlawful practice.[350]

Amazon.com, Inc. (Amazon) experienced problems with an AI employment tool because of both the "garbage in, garbage out" and machine-learning evolution problems. In 2018, Amazon had to scrap an AI recruiting tool because it showed a negative bias towards women.[351] Automation and machine learning has been the key to the e-commerce giant's dominance.[352] However, the company ran into problems when it attempted to expand machine learning into its hiring process. Its machine-learning specialists created programs that reviewed the resumes of job applicants and gave "job candidates scores ranging from one to five stars—much like shoppers rate products on Amazon."[353] Only one year into the program, "the company realized its new system was not rating candidates in a gender neutral way." The algorithms "were trained to vet applicants by observing patterns in resumes submitted to the company over a 10-year period." The system effectively "taught itself that male candidates were preferable." For example, "It penalized resumes that included the word 'women's,' as in 'women's chess club captain.'" Most concerning, there "was no guarantee that the machines would not devise other ways of sorting candidates that could prove discriminatory" even after the company edited the programs to make terms, like women, neutral in the decision process.[354]

"Concerns regarding racial or gender bias in AI have arisen in applications as varied as hiring, policing, judicial sentencing, and financial services. The application of AI to the financial services sector is particularly relevant when considering how using consumer credit information data in risk assessments could create bias in the security clearance process. "Banks have recently been pushing into AI for trade surveillance and financial crimes compliance."[355] One of the motivating factors for this push has been an effort to use this "technology to identify risks proactively through predictive analytics."[356] However, "fairness and equity is not something that an algorithm can necessarily be trained" to weigh.[357] "In a commonly noted and related example, 'American Express lowered a customer's credit limit from $10,800 to $3,800, not based on his payment history with the company, but because 'other customers who [had] used their card at establishments where [he had] recently shopped [had] a poor repayment history with American Express.'"[358] Zest AI, a leading underwriting service provider that uses algorithms to make credit decisions, has taken the position that "all data is credit data—that is, predictive analytics can take virtually any scrap of information about a person, [analyze] whether it corresponds to a characteristic of known-to-be-creditworthy people, and extrapolate accordingly."[359] "In a 2008 FTC enforcement action against CompuCredit, the FTC alleged the company deceived consumers 'by failing to disclose that consumers' credit lines would be reduced if they used their credit cards for cash advances or for certain types of transactions, including marriage counseling, or at bars and nightclubs.'"[360] If an AI algorithm is fed a large amount of consumer financial data on a security clearance holder, the algorithm could evolve to erroneously identify potential intelligence threats using discriminatory and erroneous factors.

The third problem is understanding and measuring fairness.[361] Federal agencies can "responsibly take advantage" of the ways "AI can improve on traditional human-decision-making."[362] In fact, "using AI to improve decision-making may benefit traditionally disadvantaged groups, as researchers Jon Kleinberg, Sendhil Mullainathan, and others call the 'disparate benefits from improved prediction.'"[363] Fairness in the AI context seems straightforward, but it can be difficult to implement. Developers can require "that models have equal predictive value across groups" or require "that models have equal false positive and false negative rates across groups. However, this leads to a significant challenge—different fairness definitions usually cannot be satisfied at the same time."[364] Industry leaders like Google highlight "there is no standard definition of fairness, whether decisions are made by humans or machines. Identifying appropriate fairness criteria for a system requires accounting for user experience, cultural, social, historical, political, legal, and ethical considerations …."[365] "Tech Giants" like Facebook, Amazon, Microsoft, Google, and IBM have all announced open source tools that developers

can use to examine bias and fairness in AI systems, but these tools are only as good as the criteria and factors that developers create.[366] State-of-the-art bias mitigation algorithms may help address the concerns previously identified, but federal agencies will still be left with the challenge of defining fairness when it comes to the security clearance context. Unlike in a hiring decision where a discriminatory disparate impact presents both legal and moral concerns, should mere alert or flagging systems have to follow this same definition of fairness? Decision-makers will have to wrestle with the trade-offs from modifying an algorithm to ensure fairness across groups and the insights that might be gained from better factoring in individual differences.

Even if an algorithm erroneously or discriminately identifies a clearance holder as a potential threat, proponents of using AI in the continuous evaluation process can argue that a neutral, trained adjudicator will still need to review the alert and make a decision based on the underlying information that caused the alert. However, an agency's decision to begin an investigation into a holder's continued eligibility for a security clearance is largely shielded from judicial review under discrimination laws like Title VII of the Civil Rights Act of 1964.[367] Consistent with the Supreme Court's holding in *Egan*, "the general presumption favoring judicial review 'runs aground when it encounters concerns of national security.'"[368] Future courts could hold that a machine-learning-based system administered by "appropriately trained adjudicative personnel" is largely or completely immune from judicial review.[369] Even if a trained adjudicator ultimately makes a decision that the clearance holder's continued eligibility is not at risk, the clearance holder's work may already have been interrupted by an investigation and there is no source of judicial redress for the underlying errors in the system. Courts may find ways to redress "runaway" machine learning systems under *Egan* and its progeny, but litigants would still have challenges getting access to classified or sensitive algorithms. Agencies will likely resist efforts to expose the underlying algorithms for these programs in discovery.[370] Even if litigants were to gain access to the algorithms, proof that discrimination is occurring may not be apparent, even to developers.[371] AI has incredible potential to addressing human bias in security clearance investigations, but agencies will need to address these challenges before incorporating it into the security clearance process.

It is imperative that any use of machine learning or autonomous identification system in the CE context appropriately address these three main challenges: (1) bias built into data, (2) amplification of bias as AI algorithms learn or evolve, and (3) understanding and measuring "fairness." As this technology develops, the President and the ODNI need to require agencies to report periodically the demographic data of the individuals flagged by any autonomous system in a way

that allows effective oversight of the system by Congress and the Executive. Reporting must be an essential part of any system because it is the only way to better position agencies to identify and address any disparities and ensure that the security clearance investigation process is fair. In a recent investigation by the GAO into the DoD and U.S. Coast Guard's capabilities to assess racial and gender disparities in their investigations, military justice, and personnel databases, the GAO found that neither maintained consistent information about race and ethnicity in their databases.[372] Even with these database deficiencies, the GAO "found that Black, Hispanic, and male [service members] were more likely than White or female members to be the subjects of investigations recorded in databases used by the military criminal investigative organizations, and to be tried in … courts-martial in all of the military services when controlling for attributes such as rank and education."[373] The White House's Office of Management and Budget (OMB) has federal standards for reporting race and ethnicity for all federal reporting purposes and this investigation showed the importance of using standardized reporting practices.[374] In addition, the GAO had difficulty pulling information from different databases across the different services because the services failed to accurately record information or they were unable to match records among the different databases, among other problems.[375] It is imperative that the reporting structure of a continuous evaluation system has accurate data field definitions and the databases are created in a way that allows researchers to collect, search, and provide meaningful statistical analysis. Quality information and the ability to obtain data on a timely basis are essential parts of an effective reporting system and is the only way for agencies to know whether autonomous reporting systems are operating in a non-discriminatory fashion.[376]

In addition, agencies need to develop "responsibility practices" for autonomous systems that clearly outline how systems will specifically incorporate fairness into their CE automated systems. Any machine-learning technology acquired by agencies will need to include bias-mitigation measures that effectively accomplish the goal of identifying risks while also protecting clearance holders from unfair bias. The Information Technology Industry Council, which represents many of the industry leaders in AI, published a list of principles to guide the ethical development of AI programs.[377] The principles include concepts like "robust and representative data," which includes the responsibility of understanding "the parameters and characteristics of the data, to demonstrate the recognition of potentially harmful bias, and to test for potential bias before and throughout the deployment of AI system."[378] In addition, the principles stress the importance of "interpretability," which includes findings ways "to mitigate bias, inequity, and potential harms in automated decision-making systems" using tailored approaches unique to the context of the system."[379] In February 2020, the DoD officially

adopted ethical principles for AI based on recommendations provided by the Defense Innovation Board, an independent federal advisory committee.[380] The principles, which will apply to both combat and non-combat uses of AI across all facets of the DoD, include a focus on taking "deliberate steps to minimize unintended bias."[381] In addition, they also recognize the importance of traceability and ensuring AI capabilities are developed and deployed such that relevant personnel "possess an appropriate understanding of the technology, development process, and operation methods" including "transparent and auditable methodologies, data sources, and design procedure and implementation."[382] Establishing AI responsibility practices specific to the security clearance process, derived from the principles already instituted by the DoD, will assist agencies tailor their systems to the unique needs of their continuous evaluation systems while still ensuring developers, contractors, and industry develop the systems in an ethical manner that mitigates the risk of bias. Implementing these policies along with effective reporting is the best way to prevent unfair bias or discrimination from affecting CE programs.

D. Unfair Debt Collection Practices Reporting and Education

The last piece of the security clearance process that needs attention as agencies use consumer credit information in the CE process is unfair debt collection practices affecting clearance holders. Agencies need to educate their workforces about their rights when contacted by debt collectors and create avenues for clearance holders to report deceptive and unfair debt collection tactics. In addition, agencies need to provide effective training to adjudicators and investigators that focuses on an individual's rights under the FDCPA and the potential unfair consequences of CE on debt collection practices. Although there is no published information on how unfair debt collection practices affect clearance holders or the security clearance investigation process, military personnel make up a significant percentage of the over four million individuals who hold a security clearance[383] and service members have reported more complaints about debt collection activities than the general population.[384] A debt collector cannot tell a service member's chain of command that the member owes a debt; threaten the service member with prosecution under the Uniform Code of Military Justice (UCMJ); nor "Threaten an action they are not authorized to pursue," such as revoking the service member's security clearance or reducing the member's rank.[385]

Many of the complaints by service members are directly relevant to concerns about continued eligibility for access to classified information for all clearance holders and its relation to consumer credit information.[386] "When compared to the general population who files complaints [to the CFPB], service members'

complaints are nearly *twice* as likely to be about debt collection."[387] In many of the complaints the CFPB receives, service members assert "the amount of underlying debt is inaccurate or unfair" and a significant number of complaints are about calls to third parties (including the member's chain of command) about debts, a violation of the FDCPA.[388] The CFPB has brought enforcement actions against Navy Federal Credit Union (NFCU) and an auto lender for threatening service members that they would take would take legal action against them and contact their commanding officers if they did not promptly make payment on unpaid debts to coerce them into paying, despite the fact that they were not authorized to communicate with their employers.[389] When taking action against NCFU, the CFPB specifically mentioned the concern that "consumer credit problems can result in disciplinary proceedings or lead to revocation of a security clearance."[390] In 2015, the Washington State Office of the Attorney General settled with Freedom Stores, Inc. for its unfair debt collection practices, including contacting service members' units and commanders to discuss the details surrounding their debt.[391]

On March 2, 2020, the U.S. House of Representatives unanimously passed The Fair Debt Collection Practices for Service Members Act with the express purpose of providing "enhanced protection against debt collector harassment of members of the Armed Forces."[392] The bill would have amended the FDCPA to specifically prohibit debt collectors from threatening to revoke the service member's security clearance and makes it an unfair practice to threaten that failing to "cooperate with a debt collector" will result in a revocation of the service member's security clearance.[393] It also outlined prohibitions regarding similar threats to have the service members reduced in rank or prosecuted under the UCMJ.[394] In addition, it required the GAO to study the impact that this bill will have on the timely delivery of information about these new proposed changes to the FDCPA; "military readiness; and national security, including the extent to which covered members with security clearances would be impacted by uncollected debt."[395] Although this bill proscribed debt collector practices that are already likely unfair or deceptive under the FDCPA, it was a direct response to recent cases showing that debt collectors have targeted service members with harassment and invoked the danger of losing one's security clearance to induce compliance.

Based on the above cases, the CFPB and state attorneys general have the legal tools they need to combat unfair and deceptive debt collectors under the current security clearance process, but CE will add an additional coercive effect to threats by debt collectors towards clearance holders. Since CE will use an ongoing screening process and leverage automated record checks, a debt collector who is attempting to collect a debt that is not on a clearance holder's credit report could state that the debt, whether valid or invalid, will be reported to the CRAs and be

flagged by CE programs. Consequently, a clearance holder may be more willing to agree to resolve a debt that they do not owe, is time-barred from collection based on the statute of limitations, or includes fees and charges that they do not agree with rather than face the prospect of a negative credit report entry being flagged by CE programs. This possible consequence is particularly concerning when a partial payment could "revive time-barred debts—causing legal unenforceable debt to become enforceable once more, despite the initial statute of limitations running its course."[396] For these reasons, it is imperative that agencies educate their workforces about their rights when contacted by debt collectors and create policies that allow clearance holders to report deceptive and unfair debt collection tactics to security professionals in ways that will not jeopardize their security clearances. In addition, training must be provided to adjudicators and investigators that focuses on an individual's rights under the FDCPA and the potential unfair consequences of CE on debt collection practices. The National Security Adjudicative Guidelines, which were revised in 2017, included a reasonably-based dispute as to the legitimacy of past-due debt as one the "conditions that could mitigate security concerns" with regard to financial concerns.[397] Specifically, one of the mitigating conditions is that "the individual has a reasonable basis to dispute the legitimacy of the past-due debt which is the cause of the problem and provides documented proof to substantiate the basis of the dispute or provides evidence of actions to resolve the issue."[398] Since disputing the legitimacy of a debt could take several months,[399] a clearance holder may not have "documented proof to substantiate the basis of the dispute" when a debt is first reported on a credit report and identified in an automated records check. A clearance holder should not have their continued eligibility for access to classified information placed in jeopardy until they have had full and fair opportunity to validate the legitimacy of a debt and dispute the basis or amount of the debt. Clearance holders that do not understand their rights or how their employer will handle disputed or unverified debts is more likely to pay a debt they do not owe or succumb to unfair or deceptive debt collection practices and agencies need to understand these potential consequences as they institute CE programs.

VI. Conclusion

During the Truman Administration, his loyalty program investigated more than 4.7 million federal employees for disloyalty.[400] The program came to fruition during the Cold War to protect against the "infiltration of disloyal persons" and even included provisions designed to give employees "equal protection from unfounded accusations of disloyalty."[401] However, the program had a corrosive effect on the federal workforce and "created a pervasive sense of being 'watched.'"[402] In the end, only about one in every 13,000 employees subject to investigation were

actually discharged for disloyalty.[403] The modern security clearance process is far removed from the loyalty program of the Truman era, but it is important to remember how a program created with noble goals of protecting national security can cause unnecessary and unfair burdens on federal employees and clearance holders.

Even though national security requires "any doubt whether to grant an individual access to classified information" to be "resolved in favor of the national security,"[404] clearance holders deserve a CE system that is fair, free from bias, and effective without being unduly burdensome. The ODNI can protect current clearance holders from the effects of erroneous or misleading consumer credit information by: (1) mandating an effective, centralized investigation database that prevents the reflagging of previously adjudicated issues in credit records; (2) ensuring appropriate oversight and burden sharing among agencies, CRAs, and clearance holders; (3) requiring the reporting and analysis of automated records check systems to identify potential bias or disparate impacts on protected classes and minority groups; and (4) mandating education efforts to address unfair debt collection practices.

In 2019, Brian Dunbar, the assistant director of security for ODNI's National Counterintelligence and Security Center, spoke about the change of perspective that CE will create in the security clearance investigation process.

> With near-real-time information about an employee's missed credit card payment, for example, DoD and other adjudicatory agencies will need to shift their mindset as they evaluate the trustworthiness of their workforce. I [can] find something out on you tomorrow that you did yesterday. Time is not going to be a mitigator. But what might be a mitigator and what will be in the new adjudicative model will be, what did you do about it? What outcome, what action did you take? Were you responsible? Or were you irresponsible? People have lives; people make mistakes. It's a different mindset.[405]

As federal agencies embrace CE in their security clearance and suitability investigation processes, it is imperative that they not only consider how they will judge the information they receive through CE, but that they also protect clearance holders from the negative effects of inaccurate credit information and take steps to create a system that is effective, but also fair.

Endnotes

[1] *See* Lindy Kyzer, *Government Reframing Who's a Trusted Worker as Trusted Workforce 2.0 Marks 1-Year Anniversary*, ClearanceJobs (Feb. 28, 2019), https://news.clearancejobs.com/2019/02/28/government-reframing-whos-a-trusted-worker-as-trusted-workforce-2-0-marks-1-year-anniversary/; *see also Trusted Workforce 2.0: The Future of Personnel Vetting*, 2 CDSE Pulse (U.S. Def. Counterintelligence and Sec. Agency), July 2010 at 1–2, https://www.dcsa.mil/Portals/91/Documents/about/err/CDSE_Pulse_July2021.pdf.

[2] *See* Kyzer, *supra* note 1; *The Future of Personnel Vetting*, *supra* note 1, at 1–2.

[3] Nicole Ogrysko, *The Future of Continuous Evaluation is Just About Here, and it has a Different Name*, Fed. News Network (Sept. 6, 2019, 6:15 PM), https://federalnewsnetwork.com/workforce/2019/09/the-future-of-continuous-evaluation-is-just-about-here-and-it-has-a-different-name/.

[4] *See id.*

[5] *See* David Luckey, et al., Assessing Continuous Evaluation Approaches for Insider Threats: How Can the Security Posture of the U.S. Departments and Agencies Be Improved?, RAND Corp. *x* (2019), *available at* https://www.rand.org/pubs/research_reports/RR2684.html.

[6] *See id.* at *x*.

[7] *See id.* at 52.

[8] *See* Exec. Order No. 13,467, 128 Fed. Reg. 38103, 38104 (June 30, 2008).

[9] *See* Anthony Camilli & Joshua Friedman, *WARNO: New Security Clearance Guidelines Make it More Important than ever for Servicemembers to Monitor their Credit*, U.S. Consumer Fin. Protection Bureau (Aug. 20, 2018), https://www.consumerfinance.gov/about-us/blog/warno-new-security-clearance-guidelines-make-it-more-important-ever-servicemembers-monitor-their-credit/.

[10] *See Who's Keeping Score? Holding Credit Bureaus Accountable and Repairing a Broken System: Hearing Before the H. Comm. on Fin. Servs.*, 116th Cong. 2–6 (Feb. 26 2019) (testimony of Chi Chi Wu), *available at* https://financialservices.house.gov/uploadedfiles/hhrg-116-ba00-wstate-wuc-20190226.pdf.

[11] *See* Aaron Klein, *The Real Problem with Credit Reports is the Astounding Number of Errors,* Brookings Inst. (Sept. 28, 2017), https://www.brookings.edu/research/the-real-problem-with-credit-reports-is-the-astounding-number-of-errors/.

[12] *See Recovery Underway: Defense Industry Still In Recovery Mode, but Spring May be Coming – A Comprehensive Earning Survey of Security-Cleared Professionals* 4, ClearanceJobs (June 2, 2017), http://clearance-jobs-assets.s3.amazonaws.com/customer/ClearanceJobs_2017SalarySurvey_6-2-17_CJ_NEW.pdf.

[13] *See id.* at 12.

[14] *See* Michelle D. Christensen, Cong. Research Serv., R43216, Security Clearance Process: Answers to Frequently Asked Questions 1 (Oct. 7, 2016); *see also* Exec. Order No. 10,450, 18 Fed. Reg. 2489 (Apr. 27, 1953).

[15] *See* Megan Dunn, *You're Fired!–The Role of State Courts in the Expungement of Criminal Records for Federal Security Clearance Purposes,* 71 Mo. L. Rev. 495, 502 (2006).

[16] *See* Exec. Order. No. 10,290, 3 C.F.R. § 789 (1949–1953); *see also* David C. Mayer, *Reviewing the National Security Clearance Decisions: The Clash Between Title VII and Bivens Claims*, 85 Cornell L. Rev. 786, 793–94 (2000).

[17] Exec. Order No. 9,835, 12 Fed. Reg. 1935 (Mar. 21, 1947).

[18] Harry S. Truman Library, Truman's Loyalty Program, https://www.trumanlibrary.gov/education/presidential-inquiries/trumans-loyalty-program (last visited May 12, 2020).

[19] *See* Exec. Order No. 10,501, 3 C.F.R. § 979 (1949–1953); Exec. Order No. 11,652, 3 C.F.R. § 678 (1971–1975); Exec. Order No. 12,065, 3 C.F.R. § 190 (1978); Exec. Order No. 12,356, 4.1(a), 3 C.F.R. § 174 (1982).

[20] *See* Exec. Order No. 10,450, 18 Fed. Reg. 2489 (Apr. 27, 1953).

[21] Christensen, *supra* note 14, at 3.

[22] The total number of individuals eligible for access represents a 1.2 percent decrease (50,103 fewer individuals) since October 1, 2016. *See* Off. of the Dir. of Nat'l Intelligence, Fiscal Year 2017 Annual Report on Security Clearance Determinations 5 (Aug. 27, 2018) [hereinafter 2017 Annual Report on Security Clearance Determinations], https://www.dni.gov/files/NCSC/documents/features/20180827-security-clearance-determinations.pdf.

[23] *Id.;* Exec. Order. No. 12,968, 60 Fed. Reg. 40245 (Aug. 2, 1995).

[24] Christensen, *supra* note 14, at 1.

[25] *See* Exec. Order. No. 12,968, *supra* note 23, at 40246.

[26] *Id.*

[27] The Standard Form 312 is a nondisclosure agreement used by some, but not all, federal agencies. *See, e.g.,* Off. of the Dir. of Nat'l Intelligence, Standard Form 312 (July 2013), https://www.archives.gov/files/isoo/security-forms/sf312.pdf.

[28] *See* Christensen, *supra* note 14, at 1l; *see also* 50 U.S.C. § 3161 (2020).

[29] *See* Exec. Order No. 13,526; 75 Fed. Reg. 707, 707–08 (Dec. 29, 2009).

[30] *See id.*

[31] *Id.* at 709.

[32] *Id.* at 707–08.

[33] *Id.*

[34] *See* Off. of the Dir. of Nat'l Intel., Intelligence Community Directive 703, at 2 (June 13, 2013), *available at* https://www.dni.gov/files/documents/ICD/ICD%20703.pdf.

[35] *See id*.

[36] 32 C.F.R. § 154.17 (2010).

[37] *Id.; see also* Off. of the Dir. of Nat'l Intel., Intelligence Community Directive 704 (Oct. 1, 2008), *available at* https://www.dni.gov/files/documents/ICD/ICD_704.pdf; Off. of the Dir. of Nat'l Intel., Intelligence Community Directive 906 (Oct. 17, 2015), *available at* https://www.dni.gov/files/documents/ICD/ICD906.pdf.

[38] *See* Christensen, *supra* note 14, at 6; *see also* Dep't of Def. Manual 5205.07, 8 (Apr. 5, 2018), https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/510521m_vol2.pdf; Dep't of Def. Directive 5205.07, 19 (Feb. 4, 2020). https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/520507p.pdf?ver=2020-02-04-142942-827.

[39] *See* Christensen, *supra* note 14, at 6.

[40] *See infra* Part III.

[41] *Id.; see also* 5 C.F.R. § 732.201 (2001).

[42] *See* Christensen, *supra* note 14, at 6; U.S. Off. of Per. Mgmt., Standard Form 86 (June 2017), https://www.opm.gov/forms/pdf_fill/sf86.pdf.; *see also* Exec. Order No. 12,968, 60 Fed. Reg. 40245 (Aug. 2, 1995).

[43] *See* U.S. Off. of Personnel Mgmt., Standard Form 85 (Dec. 2017), https://www.opm.gov/forms/pdf_fill/sf85p.pdf; and U.S. Off. of Personnel Mgmt., Standard Form 85P (Dec. 2017), https://www.opm.gov/forms/pdf_fill/sf85p.pdf. *See also* Lindy Kyzer, *What's the Difference Between the SF86 and SF85?,* ClearanceJobs (Mar. 8, 2018), https://news.clearancejobs.com/2018/03/08/whats-difference-sf86-sf85/.

[44] *See* U.S. Off. of Pers. Mgmt., Completing your Investigation Request in E-QIP: Guide for the Standard Form (SF) 86, 4 (July 2018), https://www.dcsa.mil/Portals/91/Documents/pv/mbi/standard-form-sf-86-guide-for-applicants.pdf.

[45] *See id.*

[46] *Id.* at 4.

[47] *See* Press Release, Defense Counterintelligence and Security Agency, Background Investigation Mission Moving (July 29, 2019), *available at* https://www.dcsa.mil/About-Us/News/News-Display/Article/1919661/background-investigation-mission-moving/.

[48] *See* U.S. Off. of Pers. Mgmt., Standard Form 86 (June 2017), https://www.opm.gov/forms/pdf_fill/sf86.pdf.

[49] *Id.* at 35, 131–33. The authorization for release of medical information complies with the Health Insurance Portability and Accountability Act of 1996 and authorizes the investigator to ask health practitioners about mental health consultations. *See* 45 C.F.R. § 160 & 164 (2013). In addition, the SF 86 includes an authorization to release "[o]ne or more reports from consumer reporting agencies" pursuant to the Fair Credit Reporting Act. *See* 15 U.S.C. § 1681b (2020).

[50] Standard Form 86, *supra* note 48.

[51] *See id.*; 18 U.S.C. § 1001 (2020).

[52] *See* Christensen, *supra* note 14, at 8 (citing U.S. Dep't. of Justice, Review of the Department's Contractor Personnel Security Process, 4 (Mar. 2013), https://oig.justice.gov/reports/2013/e1303.pdf).

[53] *See* Christensen, *supra* note 14, at 7.

[54] *Id.* at 8 (citing Off. of the Dir. of Nat'l Intel., Fiscal Year 2012 Report on Security Clearance Determinations, 5 (Jan. 2013), https://www.dni.gov/files/documents/2012%20Report%20on%20Security%20Clearance%20Determinations%20Final.pdf).

[55] *Id.* Christensen, *supra* note 14, at 7.

[56] Off. of the Dir. of Nat'l Intel., Intelligence Community Policy Guidance Number 704.1, (Oct. 2, 2008), *available at* https://www.dni.gov/files/documents/ICPG/icpg_704_1.pdf.

[57] *Id.* at 3–6.

[58] *Id.*

[59] Off. of the Dir. of Nat'l Intel., Intelligence Community Policy Guidance Number 704.6, (Feb. 4, 2015), *available at* https://www.dni.gov/files/documents/ICPG/ICPG%20704.6.pdf.

[60] *Id.* at 1.

[61] *Id.*

[62] *Id.* at 2.

[63] *Id.*

[64] *See* Christensen, *supra* note 14, at 6.

[65] 32 C.F.R. § 147.2 (1998); *see also* Exec. Order. No. 12,968, 60 Fed. Reg. 40245, 40250 (Aug. 2, 1995).

[66] 32 C.F.R. § 147.2; *see also* Exec. Order. No. 12,968.

[67] 32 C.F.R. § 147.2.

[68] *See* Kaplan v. Conyers, 733 F.3d. 1148, 1164 (Fed. Cir. 2013) (*citing* Dep't of the Navy v. Egan, 484 U.S. 518, 531 (1988)).

[69] 32 C.F.R. § 147.2; *see also* Off. of the Dir. of Nat'l Intel., Security Executive Agent Directive 4, 8–24 (June 8, 2017) [hereinafter SEAD 4], *available at* https://www.dni.gov/files/NCSC/documents/Regulations/SEAD-4-Adjudicative-Guidelines-U.pdf.

[70] Security Executive Agent Directive 4 (SEAD 4), issued by the ODNI, establishes a single common criterion for use by all executive branch agencies to use when rendering a final eligibility determination. SEAD 4 discusses the concerns raised under each of the guidelines, the "conditions that could raise a security concern and may be disqualifying," and "conditions that could mitigate security concerns." *See* SEAD 4, *supra* note 69, at 8–24.

[71] 32 C.F.R. § 147.2(d).

[72] *Id.* at (e).

[73] *Id.* at (d).

[74] SEAD 4, *supra* note 69, at 15.

[75] *See id.* at 16.

[76] *See id.*

[77] *See, e.g.,* Def. Off. of Hearings & Appeals, 2018 Industrial Security Clearance Decisions (Archive), https://doha.ogc.osd.mil/Industrial-Security-Program/Industrial-Security-Clearance-Decisions/ISCR-Hearing-Decisions/Archived-ISCR-Hearing-Decisions/2018-ISCR-Hearing-Decisions/ (last visited Aug. 19, 2021).

[78] *See id.; see also* Marko Hakamaa, *Top Reasons for Security Clearance Denial in 2018* (Dec. 20, 2018), ClearanceJobs, https://news.clearancejobs.com/2018/12/20/top-reasons-for-security-clearance-denial-in-2018/.

[79] SEAD 4, *supra* note 69, at 27.

[80] *See id.*

[81] *Id.*

[82] *Id.*

[83] *Id.*

[84] *See* Christensen, *supra* note 14, at 10; *see also* Exec. Order. No. 12,968, 60 Fed. Reg. 40245, 40252 (Aug. 2, 1995); *see, e.g.,* Off. of the Dir. of Nat'l Intel., Intelligence Community Policy Guidance Number 704.3 (Oct. 2, 2008), *available at* https://www.dni.gov/files/documents/ICPG/icpg_704_3.pdf.

[85] *See* Exec. Order. No. 12,968, *supra* note 84, at 40252. If requested, any "documents, records, and report" will be provided "to the extent the documents would be provided if requested under the Freedom of Information Act (5 U.S.C. § 552) or the Privacy Act (5 U.S.C. § 552a)." *See id.*

[86] Exec. Order 12,968, *supra* note 84, at 40252.

[87] *See id*.

[88] *See id*.

[89] *See id*.

[90] *See* 2017 Annual Report on Security Clearance Determinations, *supra* note 22, at 8.

[91] *See id.*

[92] *See id.*

[93] This represents a 0.4 percent increase in the number of clearances approved since fiscal year 2016. *See id.*

[94] *See infra* Part III.

[95] 50 U.S.C. § 3341 (2020); *see also* Exec. Order. No. 12,968, 60 Fed. Reg. 40245, 40246 (Aug. 2, 1995).

[96] By statute, periodic investigations must be completed every five years for an individual with a Top Secret clearance or access to a "highly sensitive program" and every 10 years for an individual with a secret clearance. *See* 50 U.S.C. § 3341(7). However, backlogs have stretched reinvestigation timelines for Top Secret clearances to six years. *See* Merton W. Miller, *2018 State of the Security Clearance Process* 2, ClearanceJobs (2018), https://cdn.clearancejobs.com/TheStateoftheSecurityClearanceProcess.pdf.

[97] *See* Exec. Order. No. 12,968 *supra* note, 95 at 40251.

[98] *See id.*

[99] *See, e.g.,* Dep't of the Navy v. Egan, 484 U.S. 518 (1988); High Tech Gays v. Def. Ind. Security Clearance Off., 895 F.2d 563, 577 (9th Cir. 1990); Claybrook v. Slater, 111 F.3d 904, 908 (D.C. Cir. 1997).

[100] *See Egan*, 484 U.S. at 530.

[101] *See id.* at 520.

[102] *See id.*

[103] *See id.;* John O. Shimabukuro & Jennifer A. Staman, Cong. Research Serv., R45630, Merit Systems Protection Board: A Legal Overview 1 (Mar. 25, 2019), *see also* Egan v. Dep't of the Navy, 28 M.S.P.R. 509 (1985).

[104] *See Egan*, 28 M.S.P.R. at 523.

[105] *See id.* at 527.

[106] *See id.* (citing Cafeteria Workers v. McElroy, 367 U.S. 886, 890 (1961).

[107] *See Egan*, 28 M.S.P.R. at 528.

[108] *See id*. at 529 (citing Adams v. Laird, 430 F.2d 230,239 (1969), *cert denied*, 397 U.S. 1039 (1970)).

[109] *See Egan*, 28 M.S.P.R. at 529 (citing CIA v. Sims, 471 U.S. 159, 170 (1985).

[110] *See Egan*, 28 M.S.P.R. at 529.

[111] *See* Heidi Gilchrist, *Security Clearance Conundrum: The Needs for Reform and Judicial Review*, 51 U. Rich. L. Rev. 953, 956 (May 2017).

[112] *See* Louis Fisher, *Judicial Interpretations of Egan*, LL. File No. 2010-003499 (Nov. 13, 2009), L. Library of Cong, *available at* http://www.loufisher.org/docs/ep/466.pdf.

[113] *See id.* at 10.

[114] *See id.; see, e.g.,* Hill v. Dep't of the Air Force, 844, F.2d 1407, 1409 (10th Cir. 1988); United States v. Voge, 844 F.2d 776, 779 (Fed. Cir. 1988).

[115] *See* Jamil v. Sec'y, Dep't of Def., 910 F.2d 1203, 1205–06 (4th Cir. 1990); Dormont v. Brown, 913 F.2d 1399, 1401 (9th Cir. 1990); Perez v. FBI, 71 F.3d 513, 514–15 (5th Cir. 1995).

[116] Webster v. Doe, 486 U.S. 592 (1988).

[117] *See id.* (citing Johnson v. Robison, 415 U.S. 361 (1974).)

[118] *See Webster,* 486 U.S. at 603.

[119] *See id.*

[120] *See, e.g., Jamil*, 910 F.2d at 1207; Ryan v. Reno, 168 F.3d 520 (D.C. Cir. 1999).

[121] *See* Rattigan v. Holder 689 F.3d 764, 767 (D.C. Cir. 2012); *but see* Becerra v. Dalton, 94 F.3d 145, 149 (4th Cir. 1996).

[122] *See Rattigan,* 689 F.3d at 767. The Court also highlighted that under Executive Order 12,968, a security clearance adjudication decision be "based on judgment by appropriately trained adjudicative personnel." *See* Exec. Order No. 12,968, 60 Fed. Reg. 40245 (Aug. 2, 1995).

[123] *See Rattigan,* 689 F.3d at 765–66.

[124] *See id.* at 768.

[125] *See* Heidi Gilchrist, *Security Clearance Conundrum: The Needs for Reform and Judicial Review*, 51 U. Rich. L. Rev. 953, 954 (May 2017).

[126] *See* Merton W. Miller, *2018 State of the Security Clearance Process 1*, ClearanceJobs (2018), https://cdn.clearancejobs.com/TheStateoftheSecurityClearanceProcess.pdf.

[127] *See id.*

[128] *See id.* at 4.

[129] At the time, the GAO was called the General Accounting Office. Congress changed the name to the Government Accountability Office in 2004. *See* GAO Human Capital Reform Act of 2004, Pub.L. 108-271, 118 Stat. 811 (Jul. 7, 2004).

[130] *See* H.R. Rep. No. 107-767, at 13 (2002), *available at* https://www.congress.gov/congressional-report/107th-congress/house-report/767/1 (citing U.S. Gen. Accounting Off., GAO/NSAID-00-215, DOD Personnel: More Action Needed to Address Backlog of Security Clearance Reinvestigations 1–2 (2000), https://www.gao.gov/assets/nsiad-00-215.pdf).

[131] *See* H.R. Rep. No. 107-767, at 13.

[132] *See* U.S. Gov't Accountability Off., GAO-05-207, High-Risk Series: An Update 22 (Jan. 2005), https://www.gao.gov/assets/gao-05-207.pdf.

[133] *See* U.S. Gov't Accountability Off., GAO-19-157SP, High-Risk Series: Substantial Efforts Needed to Achieve Greater Progress on High Risk Areas 170 (Mar. 2019), https://www.gao.gov/assets/gao-19-157sp.pdf.

[134] *Security Clearance Reform: Hearing Before the S. Select Comm. on Intelligence,* 116th Cong. (Jan. 22, 2020) (statement of William Evanina) [hereinafter Statement of William Evanina], *available at* https://www.odni.gov/files/documents/Newsroom/Testimonies/22_Jan_2020_SSCI_SFR_DNI-NCSC_Security_Clearance_Reform.pdf.

[135] Cross-Agency Priority (CAP) Goal Action Plan, Security Clearance, Suitability, and Credentialing Reform (Dec. 2019), https://assets.performance.gov/archives/action_plans/dec_2019_Security_Suitability.pdf.

[136] *See id.* at 5.

[137] *See* Steven Aftergood, *DNI Orders Security Clearance "Reciprocity,"* Federation of American Scientists (Dec. 12, 2018), https://fas.org/blogs/secrecy/2018/12/dni-reciprocity/.

[138] Off. of the Dir. of Nat'l Intel., Security Executive Agent Directive 7 (Nov. 9, 2018), *available at* https://www.dni.gov/files/NCSC/documents/Regulations/SEAD-7_BI_ReciprocityU.pdf.

[139] *See* Exec. Order No. 12,968, 60 Fed. Reg. 40245, 40249 (Aug. 2, 1995).

[140] Katherine L. Herbig & Peter R. Nelson, Reciprocity: A Progress Report *vii–x*, Def. Pers. Sec. Rsch. Ctr. (April 2004), https://apps.dtic.mil/docs/citations/ADA421804.

[141] Sec. Policy Reform Council, Security Clearance Reciprocity: Obstacles and Opportunities 1, Intel. and Nat'l Sec. Alliance (June 2019), https://www.insaonline.org/insa-white-paper-identifies-impediments-to-security-clearance-reciprocity.

[142] *See id.*

[143] *See id.*

[144] Off. of the Dir. of Nat'l Intel., Security Executive Agent Directive 7 (Nov. 9, 2018) [hereinafter SEAD 7], *available at* https://www.dni.gov/files/NCSC/documents/Regulations/SEAD-7_BI_ReciprocityU.pdf.

[145] *See* Security Clearance Reciprocity, *supra* note 141, at 2.

[146] *See id.*

[147] *See id.* at 4.

[148] *See* Miller, *supra* note 96, at 11.

[149] *See* Katherine L. Herbig & Peter R. Nelson, Reciprocity: A Progress Report *xi*, Def. Personnel Sec. Research Ctr. (April 2004), https://apps.dtic.mil/docs/citations/ADA421804.

[150] *See id.*

[151] *See* Derek B. Johnson, *Federal government rolls out new framework for security clearance process* (Feb. 28, 2019), Fed. Computer Week, https://fcw.com/articles/2019/02/28/security-clearance-framework-johnson.aspx.

[152] *See* 50 U.S.C. §§ 3002–3383 (2020).

[153] *See id.*

[154] *See* Off. of the Dir. of Nat'l Intel., ODNI Factsheet (Feb. 24, 2017), https://www.dni.gov/files/documents/FACTSHEET_ODNI_History_and_Background_2_24-17.pdf.

[155] *See* 50 U.S.C. § 3341(b).

[156] *See id.* § 3341(f)–(g).

[157] *See id.* § 3341(e).

[158] *See* Exec. Order No. 13,467, 128 Fed. Reg. 38103 (June 30, 2008).

[159] *See id.*

[160] *See* Exec. Order. No. 13,741, 81 Fed. Reg. 68289 (Sept. 29, 2016).

[161] *See* 10 U.S.C. § 1564 (2020).

[162] *See* Exec. Order No. 13,869, 84 Fed. Reg. 18125 (Apr. 29, 2019).

[163] *See id.* at 18125–26.

[164] Press Release, Off. of The Dir. of Nat'l Intel., The Inspector General of the Intelligence Community Addresses Security Clearance Processing Challenges (Jun. 10, 2019), https://www.dni.gov/files/ICIG/Documents/News/ICIG%20News/2019/June%2010%20-%20Security%20Clearance%20Processing%20Challenges/20190617_GAO_Press_Release.pdf.

[165] Statement of William Evanina, *supra* note 134.

[166] *See id.* at 2.

[167] *See id.*

[168] *See id.*

[169] *See id.* at 3.

[170] *See id.*

[171] *See id.*

[172] *See id.*

[173] *See id.*

[174] *See id.*

[175] *See id.*

[176] According to Tricia Stokes, the Director of Defense Vetting for DCSA, in the future "the defense and intelligence community will pivot to the term 'continuous vetting.'" *See* Lindy Kyzer, *What's the Future of the Security Clearance Process? Continuous Vetting*, ClearanceJobs (Mar. 10, 2020), https://news.clearancejobs.com/2020/03/10/whats-the-future-of-the-security-clearance-process-continuous-vetting/.

[177] *See* Exec. Order No. 13,467, 128 Fed. Reg. 38103, 38104 (June 30, 2008).

[178] *See id.*

[179] *See* Kyzer, *supra* note 176.

[180] *See id.*

[181] *See id.*

[182] S*ee* U.S. Gov't Accountability Off., GAO-18-117, Personnel Security Clearances (Nov. 2017), https://www.gao.gov/assets/690/688530.pdf.

[183] Off. of the Dir. of Nat'l Intel., Continuous Evaluation: Top 15 Frequently Asked Questions (FAQ) (Apr. 3, 2017), https://www.dni.gov/files/NCSC/documents/products/20180316-CE-FAQs.pdf.

[184] *See* Ogrysko, *supra* note 3.

[185] *See id.*

[186] *See* GAO-18-117, *supra* note 182, at 8.

[187] Specifically, Executive Order 12968, as amended, provides that an individual who has been determined to be eligible for or who currently has access to classified information shall be subject to continuous evaluation as further defined by and under standards (including, but not limited to, the frequency of such evaluation) as determined by the DNI. *See* Exec. Order No. 12,968, § 3.5, *as amended by* Exec. Order No. 13,764, 82 Fed. Reg. 8115, 8128 (Jan. 23, 2017); *see also* GAO-18-117, *supra* note 182, at 11.

[188] *See* GAO-18-117, *supra* note 182, at 11.

[189] *See* Camilli & Friedman, *supra* note; *see also* Off. of the Dir. of Nat'l Intel., *supra* note 183, at 2.

[190] *See* GAO-18-117, *supra* note 182, at 11.; U.S. Dep't of Def. Manual 5200.02, Procedures for the DoD Personnel Security Program (PSP) 72 (Apr. 3, 2016) [hereinafter DoDM 5200.02], *available at* https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/520002m.pdf?ver=2019-05-13-104126-380.

[191] *See* GAO-18-117, *supra* note 182, at 12.

[192] *See id.* at 4.

[193] *See* GAO-19-157SP, *supra* note 133, at 20; Off. of the Dir. of Nat'l Intel., Security Executive Agent Directive 6 (Jan. 12, 2018) [hereinafter SEAD 6], https://www.dni.gov/files/NCSC/documents/Regulations/SEAD-6-continuous%20evaluation-U.pdf.

[194] U.S. Consumer Fin. Prot. Bureau, Key Dimensions and Process in the U.S. Credit Reporting System (Dec. 2012), *available at* https://files.consumerfinance.gov/f/201212_cfpb_credit-reporting-white-paper.pdf.

[195] *See id.* at 2.

[196] *See id.*

[197] *See supra* Part III.

[198] *See* U.S. Consumer Fin. Prot. Bureau, *supra* note 194, at 2.

[199] *See id.* at 7; *see also* Adi Osovosky, *Symposium: The Misconception of the Consumer as Homo Economicus: A Behavioral-Economic Approach to Consumer Protection in the Credit Reporting System*, 46 Suffolk U. L. Rev. 881, 7 (2013).

[200] *See* U.S. Consumer Fin. Prot. Bureau, *supra* note 194, at 2.

[201] Jeannette N. Bennett, *Credit Bureaus: The Record Keepers*, Fed. Reserve Bank of St. Louis (Dec. 2017), https://research.stlouisfed.org/publications/page1-econ/2017/12/01/credit-bureaus-the-record-keepers/.

[202] *See id.; see also* Mikella Hurley & Julius Adebayo, *Credit Scoring in the Era of Big Data*, 18 Yale J.L. & Tech. 148, 155 (2016).

[203] *See* U.S. Consumer Fin. Prot. Bureau, *supra* note 194, at 21 & n.54.

[204] *See* Daniel J. Solove & Paul M. Schwartz, Information Privacy Law 738 (Aspen, 6th ed. 2018).

[205] *See* Cheryl R. Cooper & Darryl E. Getter, Cong. Research Serv., R44125, Consumer Credit Reporting, Credit Bureaus, Credit Scoring, and Related Policy Issues 2 (Mar. 28, 2019).

[206] *See id.*

[207] *See id.* at 4.

[208] *See id.*

[209] *See id* at 4–5.

[210] *See* 15 U.S.C. §§ 1681–1681x (2020).

[211] *See* Solove & Schwartz, *supra* note 204, at 738.

[212] *See* 15 U.S.C. § 1681.

[213] Solove & Schwartz, *supra* note 204, at 738.

[214] *See* 15 U.S.C. § 1681a.

[215] *See* Solove & Schwartz, *supra* note 204, at 739 (citing Evan Hendricks, Credit Scores and Credit Reports: How the System Really Works, What You Can Do 304 (2004)).

[216] *See* Solove & Schwartz, *supra* note 204, at 739.

[217] *See id.*

[218] *See id.*

[219] *See* 15 U.S.C. § 1681c-1.

[220] *See id.*

[221] *See id.* § 1681j.

[222] *See id.* § 1681e(b).

[223] *See id.* § 1681(a)(1).

[224] *See id.* § 1681i.

[225] *See id.* § 1681li (b)–(c).

[226] *See, e.g.,* Sarver v. Experian Info. Solutions, 390 F.3d 969, 972 (7th Cir. 2004).

[227] *See, e.g.,* Elizabeth D. De Armond, *Frothy Chaos: Modern Data Warehousing and Old-Fashioned Defamation*, 41 Val. U. L. Rev. 1061 (2007); Jeff Sovern, *The Jewel of Their Souls: Preventing Identity Theft Through Loss Allocation Rules*, 64 U. Pitt. L. Rev. 343 (2003).

[228] *See* 15 U.S.C. § 11681h.

[229] U.S. Dep't of Justice., Victims of Identity Theft, 2016 (Jan. 2019), *available at* https://www.bjs.gov/content/pub/pdf/vit16.pdf.

[230] *See id.* at 1.

[231] *See id.* at 16.

[232] *See id.* at 11–12.

[233] Solove & Schwartz, *supra* note 204, at 764.

[234] Daniel J. Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability*, 54 Hastings L.J. 1227, 1255–56 (2003).

[235] *See id.* at 1256.

[236] *See* Solove & Schwartz, *supra* note 204, at 780 (citing Lynn M. LoPucki, *Human Identification Theory and the Identity Theft Problem*, 80 Tex. L. Rev. 89, 94 (2001)).

[237] *See* U.S. Consumer Fin. Prot. Bureau, 11 Monthly Complaint Report (May 2016), *available at* https://files.consumerfinance.gov/f/documents/201605_cfpb_monthly-complaint-report-vol-11.pdf.

[238] U.S. Fed. Trade Comm'n Report to Congress Under Section 319 of the Fair and Accurate Credit Transactions Act of 2003 (Jan. 2015), https://files.consumerfinance.gov/f/201212_cfpb_credit-reporting-white-paper.pdf.

[239] Chi Chi Wu, *supra* note 10.

[240] *See id.* at 4–5.

[241] Klein, *supra* note 11.

[242] Nat'l Consumer L. Ctr., Automated Justice: How a Mechanized Dispute System Frustrates Consumers Seeking to Fix Errors in Their Credit Reports 2 (Jan. 2009), https://www.nclc.org/images/pdf/pr-reports/report-automated_injustice.pdf.

[243] Bobby Allen, *How the Careless Errors of Credit Reporting Agencies are Ruining People's Lives*, Wash. Post (Sept. 8, 2016), https://www.washingtonpost.com/posteverything/wp/2016/09/08/how-the-careless-errors-of-credit-reporting-agencies-are-ruining-peoples-lives/.

[244] *See id.; see also* Press Release, N.Y. State Off. Of the Att'y Gen., A.G. Schneiderman Announces Groundbreaking Consumer Protection Settlement With The Three National Credit Reporting Agencies (Mar. 9, 2015), *available at* https://ag.ny.gov/press-release/2015/ag-schneiderman-announces-groundbreaking-consumer-protection-settlement-three.

[245] *See* Chi Chi Wu, *supra* note 10, at 6.

[246] *See* U.S. Consumer Fin. Prot. Bureau, Consumer Response Annual Report 7 (Mar. 2017), *available at* https://s3.amazonaws.com/files.consumerfinance.gov/f/documents/201703_cfpb_Consumer-Response-Annual-Report-2016.pdf.

[247] Lisa Stifler, *Debt in the Courts: The Scourge of Abusive Debt Collection Litigation and Possible Policy Solutions*, 11 Harv. L. & Pol'y Rev. 91, 94 (2017).

[248] *See* 15 U.S.C. §§ 1692–1692p (2020).

[249] *See id.*

[250] *See id.* § 1692k.

[251] *See id.* at § 1692a(6).

[252] *See* U.S. Fed. Trade Comm'n The Structure and Practices of the Debt Buying Industry (Jan. 2013), *available at* https://www.ftc.gov/sites/default/files/documents/reports/structure-and-practices-debt-buying-industry/debtbuyingreport.pdf.

[253] *See* U.S. Consumer Fin. Prot. Bureau, Fair Debt Collection Practices Act: Annual Report 2020, 24 (Mar. 2020), https://files.consumerfinance.gov/f/documents/cfpb_fdcpa_annual-report-congress_03-2020.pdf; Letter from April J. Tabor, Acting Sec., U.S. Fed. Trade Commission, to Kathleen L. Kraninger, Dir., U.S. Consumer Fin. Prot. Bureau (Feb. 19, 2020), *available at,* https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-enforcement-fair-debt-collection-practices-act-calendar-2019-report-bureau/ftc_annual_report_re_fdcpa.pdf.

[254] *See* U.S. Fed. Trade Comm'n, Debt Collection, https://www.ftc.gov/news-events/media-resources/consumer-finance/debt-collection (last visited Apr. 24, 2020).

[255] *See* U.S. Consumer Fin. Prot. Bureau, *supra* note 253, at 13.

[256] *See id.* at 14.

[257] *See* U.S. Fed. Trade Comm'n, *supra* note 252, at *i*.

[258] *See id.*

[259] *See* U.S. Consumer Fin. Prot. Bureau, *supra* note 253, at 14.

[260] *See id.*

[261] *See id.* at 16.

[262] *See* Press Release, Consumers Union, Report by the FTC and CFPB shows debt collection abuses remain a top consumer complaint (Mar. 21, 2018), https://advocacy.consumerreports.org/press_release/report-by-the-ftc-and-cfpb-shows-debt-collection-abuses-remain-a-top-consumer-complaint/.

[263] *See id.*

[264] *See* 15 U.S.C. § 1692g (2020).

[265] *See id.* § 1692c.

[266] *See id.*

[267] U.S. Fed. Trade Comm'n, *supra* note 254.

[268] John D. Fish, *"Unfair or Unconscionable:" A New Approach to Time-Barred Debt Collection under the FDCPA*, 86 U. Chi. L. Rev. 1941 (Nov. 2019).

[269] *See id.*

[270] *See id.*

[271] *See id.*

[272] *See* 15 U.S.C. § 1681c (2020).

[273] *See* Off. of the Dir. of Nat'l Intel., *supra* note 183.

[274] *See id.*

[275] *See* Aftergood, *supra* note 137.

[276] However, it is also possible a security professional could file an incident report or similar notification in this system that the clearance holder is not aware of after the security professional is alerted to negative, but erroneous, consumer credit information. If this erroneous credit information is not addressed and the individual is never notified, the incident report could potentially result in another agency relying upon it to deny the individual a security clearance. This could be a serious problem if the information no longer appears on the consumer's credit report and the individual has no reason to dispute it. For this reason, any database must allow a clearance holder to view all flagged consumer credit information.

[277] In addition, agencies also engage in "reciprocal revocations" of security clearances. Reciprocal revocations often occur when an individual with a security clearance granted by one agency seeks additional access to certain classified information from another agency and is denied access. In some circumstances, the individual's employing agency will reciprocally revoke the individual's original clearance based solely on the other agency's denial. *See, e.g.,* Romero v. Dep't of Def., 527 F.3d 1324, 1325–29 (Fed. Cir. 2008). As a result, a revocation or suspension of an individual's access to certain classified information by another agency could also result in the suspension or revocation of her underlying security clearance.

[278] *See* Ogrysko, *supra* note 3.

[279] *See* Aftergood, *supra* note 137.

[280] *See id.* (quoting Herbig & Nelson, *supra* note 140).

[281] SEAD 7, *supra* note 144.

[282] *See id.* at 3–4.

[283] *See id.* at 3.

[284] *See id.*; *see also* Lindy Kyzer, *Your Security Clearance Records: Making the Move from JPAS to DISS*, ClearanceJobs (Dec. 21, 2020), https://news.clearancejobs.com/2020/12/21/your-security-clearance-records-making-the-move-from-jpas-to-diss/.

[285] *See* Press Release, Def, Counterintelligence and Sec. Agency, DISS Release 13.2 (Nov. 17, 2020), *available at* https://www.dcsa.mil/About-Us/News/News-Display/Article/2417236/diss-release-132/.

[286] *See* Off. of the Dir. of Nat'l Intel., Intelligence Community Policy Guidance Number 704.5 (Oct. 2, 2008), *available at* https://www.dni.gov/files/documents/ICPG/icpg_704_5.pdf; *see* Michael Adams, *Why the OPM Hack is Far Worse Than You Imagine*, Lawfare Blog (Mar. 11, 2016, 10:00 AM), https://www.lawfareblog.com/why-opm-hack-far-worse-you-imagine.

[287] *See* Intel. & Nat'l Sec. All., Security Clearance Reciprocity: Obstacles and Opportunities (June 2019), https://www.insaonline.org/wp-content/uploads/2019/06/Security_Clearance_Reciprocity_Obstacles_and_Opportunities.pdf.

[288] *Id.* at 9.

[289] *Id.*

[290] *See id.* at 8.

[291] Def. Counterintelligence and Sec. Agency, *What is NBIS?*, https://www.dcsa.mil/is/nbis/ (last visited Aug. 7, 2021).

[292] *See* Letter from Jason Levine, Dir. Congressional, Legislative & Intergov't Affairs, U.S. Off. of Pers. Mgmt. to Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform (Aug. 21, 2015) ("The aggregate number of individuals impacted by the breach totals 22.1 million."); Majority Staff of Comm. on Oversight & Gov't Reform, 114th Cong., Data Breach: How the Government Jeopardized Our National Security for More than a Generation (Sept. 7, 2016), *available at* https://republicans-oversight.house.gov/wp-content/uploads/2016/09/The-OPM-Data-Breach-How-the-Government-Jeopardized-Our-National-Security-for-More-than-a-Generation.pdf.

[293] Ellen Nakashima & Adam Goldman, *CIA Pulled Officers from Beijing after Breach of Federal Personnel Records*, Wash. Post (Sept. 29, 2015), https://www.washingtonpost.com/world/national-security/cia-pulled-officers-from-beijing-after-breach-of-federal-personnel-records/2015/09/29/1f78943c-66d1-11e5-9ef3-fde182507eac_story.html.

[294] *See OPM Data Breach, Hearing Before the H. Comm. on Oversight & Gov't Reform,* 114th Cong. 86 (June 16, 2015), *available at* https://republicans-oversight.house.gov/hearing/opm-data-breach/.

[295] Majority Staff of Comm. on Oversight & Gov't Reform, *supra* note 292, at *iii*.

[296] Jason Chaffetz, *The Breach We Could Have Avoided*, The Hill (Sept. 30, 2015, 7:56 PM), https://thehill.com/special-reports/data-security-october-1-2015/255563-the-breach-we-could-have-avoided.

[297] *Id.*

[298] *Id.*

[299] Nakashima & Goldman, *supra* note 293.

[300] *Id.*

[301] *See* Rachel Weiner & Derek Hawkins, *Hackers Stole Federal Workers' Information Four Years Ago. Now We Know What Criminals Did With It.*, Wash. Post (June 19, 2018), https://www.washingtonpost.com/local/public-safety/hackers-stole-feds-information-four-years-ago-now-we-know-what-criminals-did-with-it/2018/06/19/f42ff2b2-73d3-11e8-805c-4b67019fcfe4_story.html; Derek Hawkins, *The Cybersecurity 202: 'A Wake Up Call.' OPM Data Stolen Years Ago Surfacing Now in Financial Fraud Case,* Wash. Post (June 20, 2018), https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/06/20/the-cybersecurity-202-a-wake-up-call-opm-data-stolen-years-ago-surfacing-now-in-financial-fraud-case/5b2924ca1b326b3967989b66/.

[302] *See id.*

[303] Majority Staff of Comm. on Oversight & Gov't Reform, 114th Cong., Data Breach: How the Government Jeopardized Our National Security for More than a Generation *vii* & 26 (Sept. 7, 2016), *available at* https://republicans-oversight.house.gov/wp-content/uploads/2016/09/The-OPM-Data-Breach-How-the-Government-Jeopardized-Our-National-Security-for-More-than-a-Generation.pdf.

[304] *See id.*

[305] *See* 15 U.S.C. § 1681i(b) (2020).

[306] *See id.* § 1681i.

[307] *Id.* § 1681i(b).

[308] *Id.*

[309] *Id.* § 1681i(c).

[310] The Privacy Act of 1974, as amended, provides an individual the ability to seek access to and amend any record pertaining to him. 5 U.S.C. § 552a(d). However, the Act also permits the head of an agency to exempt a system of records within the agency from many of the Act's requirements under specific circumstances. See *id.* § 552a(j)–(k). Intelligence agencies customarily rely on one or more of these exemptions to wholly preclude amendment requests for records related to security clearances. *See, e.g.,* Personnel Vetting Records System, 83 Fed. Reg. 52420, 52426 (Oct. 17, 2018). Accordingly, agencies will need to ensure they modify any exemptions from the Privacy Act for the system used to record this information to permit disclosure and amendment of the records.

[311] *See* Off. of the Dir. of Nat'l Intel., *supra* note 183.

[312] *Id.*

[313] Off. of the Dir. of Nat'l Intel., *supra* note 310.

[314] SEAD 6, *supra* note 193.

[315] *See id.* at 3.

[316] *See* DoDM 5200.02, *supra* note 190, at *72*.

[317] *See* Woodrow Hartzog, Gregory Conti & Lisa Shay, *Inefficiently Automated Law Enforcement*, 2015 Mich. St. L. Rev. 1763 (Apr. 28, 2016).

[318] *See supra* Part II.

[319] *See supra* Part IV.

[320] *See* Off. of the Dir. of Nat'l Intel. & U.S. Off. of Pers. Mgmt., Fact Sheet: Transforming Federal Personnel Vetting (Feb. 3, 2020).

[321] *See* Off. of the Dir. of Nat'l Intel., *supra* note 183, at 2-3.

[322] *See* SEAD 6, *supra* note 193.

[323] *See* Sarver v. Experian Info. Solutions, 390 F.3d 969 (7th Cir. 2004) (citing Cahlin v. General Motors Acceptance Corp., 936 F.2d 1151, 1156 (11th Cir. 1991); *see also* Crabill v. Trans Union, L.L.C., 259 F.3d 662 (7th Cir. 2011).

[324] *See* Elizabeth D. De. Arnold, *Frothy Chaos: Modern Data Warehousing and Old-Fashioned Defamation*, 41 Val. U. L. Rev. 1061, 1099–1102, 1108 (2007).

[325] *See* Sarver, *supra* note 322, at 972 (citing Henson v. CSC Credit Servs., 29 F.3d 280 (7th Cir. 1994)).

[326] LoPucki, *supra* note 236, at 94.

[327] *See* Solove, *supra* note 233; Lynn M. LoPucki, *Did Privacy Cause Identity Theft?*, 54 Hastings L.J. 1277 (2003).

[328] Under the FCRA, furnishers of information are currently only prohibited from "[r]eporting information with actual knowledge of errors" or "[r]eporting information after notice and confirmation of errors." 15 U.S.C. § 1681s-2 (2020).

[329] *See* Press Release, U.S. Off. of Mgmt., OPM, DoD Announce Identity Theft Protection and Credit Monitoring Contract (Sept. 1, 2015), *available at* https://www.opm.gov/news/releases/2015/09/opm-dod-announce-identity-theft-protection-and-credit-monitoring-contract/.

[330] *Id.*

[331] *See* 15 U.S.C. § 1681j.

[332] *See* SEAD 6, *supra* note 193.

[333] *See* John Bowers, *The Pentagon Wants to Streamline Security Clearances by Using AI. That's a Dangerous Idea*, Just Security (Apr. 8, 2019), https://www.justsecurity.org/63539/the-pentagon-wants-to-streamline-security-clearances-by-using-ai-thats-a-dangerous-idea/; Patrick Tucker, *The US Military Is Creating the Future of Employee Monitoring*, Defense One (Mar. 26, 2019), https://www.defenseone.com/technology/2019/03/us-military-creating-future-employee-monitoring/155824/.

[334] *See* Tucker, *supra* note 333.

[335] *See* Bowers, *supra* note 333.

[336] *See id.* (citing Julia Angwin et al., *Machine Bias*, ProPublica (May 23, 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing).

[337] *See* James Manyika, Jake Silberg & Brittany Presten, *What Do We Do About the Biases in AI?,* Harv. Bus. Rev. (Oct. 25, 2019), https://hbr.org/2019/10/what-do-we-do-about-the-biases-in-ai.

[338] *See id.*

[339] *See id.*; John Villasenor, *Artificial Intelligence and bias: Four Key Challenges*, Brookings Inst. (Jan. 3, 2019), https://www.brookings.edu/blog/techtank/2019/01/03/artificial-intelligence-and-bias-four-key-challenges/.

[340] *See* Villasenor, *supra* note 339.

[341] *See* Kristin N. Johnson, *Automating the Risk of Bias*, 87 Geo. Wash. L. Rev. 1214, 1222 (2019).

[342] *See* Villasenor, *supra* note 339; *see also* Kaveh Waddell, *How Algorithms Can Bring Down Minorities' Credit Scores*, The Atlantic (Dec. 2, 2016), https://www.theatlantic.com/technology/archive/2016/12/how-algorithms-can-bring-down-minorities-credit-scores/509333/.

[343] *See* Villasenor, *supra* note 339.

[344] *See id.*

[345] *See id.*

[346] Johnson, *supra* note 341, at 1223.

[347] *See id.*

[348] Andre Perry & David Harshbarger, *America's formerly redlined neighborhoods have changed, and so much solutions to rectify them*, Brookings Inst. (Oct. 14, 2019), https://www.brookings.edu/research/americas-formerly-redlines-areas-changed-so-must-solutions/.

[349] *Id.*; *see also* Bruce Mitchell & Juan Franco, *HOLC "Redlining" Maps: The Persistent Structure of Segregation and Economic Inequality*, Nat'l Community Reinvestment Coalition, (2018), https://ncrc.org/wp-content/uploads/dlm_uploads/2018/02/NCRC-Research-HOLC-10.pdf.

[350] *See* Villasenor, *supra* note 339.

[351] Jeffrey Dastin, *Amazon Scraps Secret AI Recruiting Tool that Showed Bias Against Women*, Reuters (Oct. 8, 2018), https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G.

[352] *See id.*

[353] *See id.*

[354] *See id.*

[355] *See* Andrew Waxman, *BankThink: AI Can Help Banks Make Better Decisions, But it Doesn't Remove Bias*, American Banker (June 5 2018), https://www.americanbanker.com/opinion/ai-can-help-banks-make-better-decisions-but-it-doesnt-remove-bias.

[356] *Id.*

[357] *Id.*

[358] *See* Matthew A. Bruckner, *Fintech's Promises and Perils: The Promise and Perils of Algorithmic Lender's Use of Big Data*, 93 Chi.-Kent L. Rev. 3, 28 (2018).

[359] *See id.* at 15.

[360] *Id.* at 47.

[361] *See* Manyika, Silberg & Presten, *supra* note 337.

[362] *Id.*

[363] *See id.*; *see also* Jon Kleinberg et al., *Human Decisions and Machine Predictions* (Nat'l Bureau of Econ. Research, Working Paper No. 23180, 2017).

[364] Manyika, *supra* note 337.

[365] Google, Responsible AI Practices, https://ai.google/responsibilities/responsible-ai-practices/ (last visited Mar. 28, 2020).

[366] *See* Paul Teich, *Artificial Intelligence Can Reinforce Bias, Cloud Giants Announce Tools for AI Fairness*, Forbes (Sept. 24, 2018), https://www.forbes.com/sites/paulteich/2018/09/24/artificial-intelligence-can-reinforce-bias-cloud-giants-announce-tools-for-ai-fairness/?sh=56bed2389d21.

[367] *See* Rattigan v. Holder, 689 F.3d 764 (D.C. Cir. 2012).

[368] *See id.* at 767 (citing Dep't of the Navy v. Egan, 484 U.S. 518, 531 (1988)).

[369] *See id.*

[370] For example, the government can resist court-order disclosure of information during litigation pursuant to the state secrets privilege if there is a reasonable danger that such disclosure would harm the national security of the United States. *See* United States v. Reynolds, 345 U.S. 1 (1953); Edward C. Liu, Cong. Research Serv., R40603, The State Secrets Privilege and Other Limits on Litigation Involving Classified Information (May 8, 2009).

[371] *See* Villasenor, *supra* note 339.

[372] *See* U.S. Gov't Accountability Off., GAO-19-344, Military Justice: DOD and the Coast Guard Need to Improve Their Capabilities to Assess Racial and Gender Disparities (May 2019), *available at* https://www.gao.gov/assets/gao-19-344.pdf.

[373] *Id.* at 40.

[374] *See id.* at 4.

[375] *Id.* at 77-81.

[376] *See* U.S. Gov't Accountability Off., GAO-14-704G, Standards for Internal Control in the Federal Government (Sept. 2014), *available at* https://www.gao.gov/assets/670/665712.pdf.

[377] *See* Info. Tech. Indus. Council, AI Policy Principles (Oct. 24, 2017), https://www.itic.org/dotAsset/50ed66d5-404d-40bb-a8ae-9eeeef55aa76.pdf.

[378] *See id.* at 3.

[379] *Id.*

[380] *See* Press Release, U.S. Dep't of Def., DOD Adopts Ethical Principles for Artificial Intelligence (Feb. 24, 2020), *available at* https://www.defense.gov/Newsroom/Releases/Release/Article/2091996/dod-adopts-ethical-principles-for-artificial-intelligence/; *see also* Def. Innovation Bd., AI Principles: Recommendations on the Ethical Use of Artificial Intelligence by the Department of Defense (Oct. 31 2019), https://media.defense.gov/2019/oct/31/2002204458/-1/-1/0/dib_ai_principles_primary_document.pdf.

[381] *See id.* at 8.

[382] *See id.*

[383] *See* Off. of the Dir. of Nat'l Intel., Fiscal Year 2017 Annual Report on Security Clearance Determinations 5 (Aug. 27, 2018), https://www.dni.gov/files/NCSC/documents/features/20180827-security-clearance-determinations.pdf; *see also* DoDM 5200.02, *supra* note 190.

[384] *See* U.S. Consumer Fin. Prot. Bureau, Servicemembers 2015: A Year in Review 9 (Mar. 2016), https://files.consumerfinance.gov/f/201603_cfpb_snapshot-of-complaints-received-from-servicemembers-veterans-and-their-families.pdf.

[385] *See* U.S. Consumer Fin. Prot. Bureau, Servicemembers: Know your rights when a debt collector calls (Sept. 2016), https://files.consumerfinance.gov/f/CFPB-Servicemembers-Know-Your-Rights-Handout-Debt-Collection.pdf.

[386] *See id.* at 2.

[387] U.S. Consumer Fin. Prot. Bureau, *supra* note 384, at 9.

[388] *See id.*;15 U.S.C. § 1692c(b) (2020).

[389] *See* U.S. Consumer Fin. Prot. Bureau, *supra* note 384, at 30; *see also* Navy Federal Credit Union, Consent Order, CFPB No. 2016-CFPB-0024 (Oct. 11, 2016), *available at* https://files.consumerfinance.gov/f/documents/102016_cfpb_NavyFederalConsentOrder.pdf.

[390] *See* Press Release, U.S. Consumer Fin. Prot. Bureau, CFPB Orders Navy Federal Credit Union to Pay $28.5 Million for Improper Debt Collection Actions (Oct. 11, 2016), *available at* https://www.consumerfinance.gov/about-us/newsroom/cfpb-orders-navy-federal-credit-union-pay-285-million-improper-debt-collection-actions/.

[391] *See* Press Release, Wash. State Off. of the Att'y Gen., AG Resolves Investigation Into Debt Collection, Deceptive Ads from Military-Centric Retailer (Oct. 23, 2015), *available at* https://www.atg.wa.gov/news/news-releases/ag-resolves-investigation-debt-collection-deceptive-ads-military-centric-retailer.

[392] *See* Fair Debt Collection Practices for Service Members Act, H.R. 5003, 116th Cong. (2020), *available at* https://www.congress.gov/bill/116th-congress/house-bill/5003/text?r=2&s=1.

[393] *See id.* at § 2.

[394] *See id.*

[395] *Id.* at § 3.

[396] *See* Fish, *supra* note 268, at 1946; *see also* Lauren Goldberg, *Dealing in Debt: The High-Stakes World of Debt Collection after FDCPA,* 79 S. Cal. L. Rev. 711, 729 (2006)*;* Lisa Stifler, *Debt in the Courts: The Scourge of Abusive Debt Collection Litigation and Possible Policy Solutions*, 11 Harv. L. & Pol. Rev. 91, 103 (2017).

[397] *See* SEAD 4, *supra* note 69, at 16; *see also* Def. Sec. Serv., 2017 National Security Adjudicative Guidelines Job Aid 19 (May 15, 2017), *available at* https://www.cdse.edu/documents/cdse/2017-Adjudicative-Guidelines.pdf.

[398] *See* SEAD 4, *supra* note 69, at 16; Def. Sec. Serv., *supra* note 397, at 19.

[399] The FDCPA sets requirements and timelines for consumers seeking validation of a debt and disputing the debt. *See* 15 U.S.C. § 1692g (2020).

[400] *See* Geoffrey Stone, Perilous Times: Free Speech in Wartime from the Sedition Act of 1798 to the War on Terrorism 348–51(Norton 2004).

[401] *See* Exec. Order No. 9,835, 12 Fed. Reg. 1935 (Mar. 21, 1947).

[402] *See* Geoffrey Stone, *supra* note 400, at 350.

[403] *See id*. at 349.

[404] *See* 32 C.F.R. § 147.2 (1998); *see also* Exec. Order. No. 12,968, 60 Fed. Reg. 40245, 40250 (Aug. 2, 1995).

[405] *See* Ogrysko, *supra* note 3.