That Escalated Quickly: The Cyber-ASAT Conundrum

*P.J. Blount**

I. Introduction

In the 1996 movie Independence Day, we find Will Smith and Jeff Goldblum fighting off an unexpected invasion of aliens. The movie's climax shows the outgunned pair saving the world by infecting the alien spacecraft's computer system with a virus written by Goldblum's character. While this scene leaves many a viewer wondering how Goldblum even knew what operating system he was writing code for, the plot twist holds an important message about digitization of which we may only now be beginning to understand the deeper ramifications. The lesson is a simple one: digitization allows for the interconnection and interaction of diverse systems.

This simple lesson is at the core of this paper, which seeks to understand how cyber-technologies are changing the space security environment. It argues that digital networking has resulted in changes that require us to reevaluate the nature of both legal and strategic limitations on states in relation to the use of anti-satellite (ASAT) technology. This paper contends that the introduction of cyber-technologies is changing the limitations that have traditionally restrained states in the development and use of ASAT technologies.

This paper will proceed as follows. First, it will address how and why cyber-technologies have had such a dramatic effect in changing social interactions, with an emphasis on on interactions between states. Second, this paper will analyze the legal framework surrounding ASATs and summarize the bounds of this weak framework. Next, this paper will analyze the strategic limitations that cause states to refrain from the use of ASATs and why these limitations have historically been effective. Finally, this paper will show that cyberspace technologies create a conundrum for those seeking to limit ASAT technologies by states, because it allows for the development of weapons that fall outside the bounds of both legal and strategic limitations.

* University of Luxembourg.

II. Recoded interactions

One of the chief rolls of the law is to encode how social interactions will unfold. Indeed, the law sets definite bounds on how individuals, commercial and noncommercial entities, and governments interact with each other. While the law sets bounds for which there is a formal penalty for violating, the law is not the only mediator of social interactions. For instance, social norms help to set regular behavioral patterns, the breach of which results in informal penalties.

Central to this paper though is how technology creates bounds to social interactions, and how changes in technologies can result in shifts in the boundaries of interactions by opening up new possibilities. This idea is easily seen in the rapid development of communication technologies in the last 30 years. The transition from voice calls over physical telephone lines to text based messaging via mobile devices has led to numerous changes in how individuals interact. For instance, SMS messaging has led to development of new language and grammar styles that even incorporate pictograms (in the form of emoticons and emojis). It has also changed the immediacy of communication by furthering the trend of shortening the temporal distance between message and response. This new medium changes the way in which individuals perceive the social interaction by imparting it with ambiguity (e.g. what does the eggplant emoji mean?) and immediacy (e.g. why hasn't she responded to my message yet?).

This SMS example may seem more suited to a paper investigating the sociology of dating in a technological world, but it is indicative of other technological changes. Technology has consistently reformed the way in which international relations among states unfold, in particular with respect to temporal aspects. A salient pre-cyber example of this is the development of intercontinental ballistic missiles (ICBM), which shortened the temporal delay between the initiation of an attack by a state to its impact on another state. Before the ICBM, a nuclear attack would have been carried out by easily detectable long-range bombers that would need a significant amount of time to reach their target allowing for time to prepare for and respond to such an attack. The development of ICBMs meant that the time between deployment and impact was shortened to mere hours thereby limiting the target's options for response.

Technology's effects change the way in which states interact in the same way that it changes the way in which people use technology to date. Foreign policy now unfolds on Twitter as world leaders make announcements and troll each other. Foreign interference in the political systems of other states has become commonplace as states leverage social media. Espionage is now the domain of the skilled computer operator rather than the covert operative seeking out microfilm. And cyberweapons have changed the way in which states calculate the costs and benefits of engaging militarily with other states.

These changes have become more pronounced as technology advances. Indeed, as the world becomes more wired the ability to communicate with everything has increased. As Internet of Things (IoT) technology has proliferated, so has the ability of cyber actors to reach across space and interact, whether for good or for bad, with the real-world environment. Indeed, it is increasingly commonplace for an individual to be able to dim a lightbulb or adjust their thermostat from a mobile device anywhere in the world. Similarly, though, it has become possible for states to use these technologies to manifest change in other states, such as the cases of Stuxnet and power station hacking in the Ukraine illustrate. Indeed, the fanciful use of a computer virus by Jeff Goldblum in *Independence Day* seems less fanciful in light of the way in which cyberspace allows a variety of systems to interconnect and interact.

The introduction of the Internet and the proliferation of cyber technologies has resulted in massive changes to how social interactions unfold. These changes affect the ability of the rule of law and strategic restraint to limit nations in their interactions and open space for new types of interactions.

III. ASAT Law

In order to understand how cyberspace changes the math on ASAT technologies, we must first establish the traditional limitations on ASAT technologies. This section will analyze the legal framework that restrains ASAT technologies. The core argument here is that the legal regime provides a relatively weak framework for limiting ASATs.

The primary limitation on ASATs is the ban on the use and deployment of nuclear weapons in outer space. This ban stems from two treaty provisions. First, the Partial Test Ban Treaty of 1963 prohibits states from causing nuclear explosions in space. This is an important limitation because a nuclear explosion causes an electromagnetic pulse (EMP), which can interfere with and disable satellites in orbit. This legal prohibition is built on in the Outer Space Treaty, Article IV, which bans states from stationing nuclear weapons in space. While the Article IV prohibition was intended to avoid crisis instability that would result from nuclear weapons targeting the terrestrial sphere, it also bolsters the prohibition on nuclear ASATS instituted in the Partial Test Ban Treaty. Article IV is not a complete prohibition of weapons in orbit. Its language is sufficiently narrow that conventional weapons stationed in space are still legal under its terms, as it only provides for a complete ban of all weapons on the Moon and other celestial bodies.

The next limitation is based on the complimentary notions of free access and non-interference. The first of these, free access, is a product of Article I of the Outer Space Treaty, which effectively gives all states a right to access, explore, and use outer space. This principle is complimented by the principle of non-interference, which is found in Article IX of the Outer Space Treaty.

Article IX requires states to act with "due regard" for the activities of other states and gives them an obligation and right to request consultations when they think they may be the source or subject of "harmful interference" with space activities. It should be noted that Article IX does not directly prohibit a state from engaging in harmful interference, which may in some cases be acceptable, for instance as an act of legitimate self-defense under Article 51 of the UN Charter. Instead of a prohibition, Article IX imposes a heightened duty to communicate with other states in situations in which harmful interference is a possibility.

In addition to the Outer Space Treaty, the non-interference principle was established in a series of bilateral arms control agreements between the United States and the USSR (and later Russia). In these agreements the method for verification of compliance was to be by "national technical means" (NTM), and the states were prohibited from "interference with national technical means" of the other state. This served as a strong prohibition on the use of ASAT technology by these two states, especially in light of the fact that it would have been impossible for either to distinguish between the other's NTM and non-NTM satellites. While some of these agreements are still in place and serve as a limitation between the US and Russia, their core weakness is that they are bilateral agreements that only provide legal limitations between these two states.

The final set of legal limitations can be found in the law of war. This category can be subdivided into the law of the use of force and the law of international armed conflict. The first of these constitutes the limitations on when a state may use military force against another state. In general there is a prohibition on the use of force under Article 2(4) of the UN Charter, but exceptions are made in cases of UN Security Council authorization (Article 42) and Self-Defense (Article 51). The Charter places no limitations on the development of weapons for defensive purposes and therefore places no limitations on the development of ASAT weapons, but it does limit when they can be used to non-aggressive purposes.

The law of international armed conflict is premised on the idea that states do not have unlimited recourse to methods and means of warfare. Instead, states are limited to weapons that can be targeted on military objectives and do not cause unnecessary damage to civilians and civilian objects. It should be noted that the law of armed conflict does place legal limits on the use of some specific weapons, but none of these prohibitions have significant implications for ASATs. The primary effect of the rules of armed conflict is to limit weapons that create and undue amount of debris. This limitations springs from two principles. The first is the principle of discrimination, which requires states to distinguish between civilian and military objects and to target solely military targets. Weapons that cannot be limited to targeting military objects are inherently illegal. In the context of space, ASAT weapons that use kinetic force to destroy a satellite thereby causing a field of debris

that could damage civilian satellites or satellites belonging to neutral parties may be illegal. The second principle is that states should not use weapons that cause long-term damage to the environment. This again means that ASAT weapons that result in large amounts of debris may be illegal. In both cases, these types of ASATs may only be illegal based on how they are used. For instance, if the ASAT is used in a distant orbit that does not risk damage to civilian satellites, then the first principle may not apply, if it is used in a low orbit that allows the debris to quickly deorbit, then the second principle may not apply. A final caveat on these rules is that they only apply when there is an international armed conflict, and not during times of peace. This means that these rules do not apply to ASAT testing, though there are nonbinding debris mitigation rules that encourage states to not intentionally destroy a satellite in orbit.

In sum, there is no clear legal prohibition on the development or use of ASAT weapons, though there are limiting principles in the legal regime. These limiting principles are actually quite weak (aside from the prohibition on nuclear ASATS) in terms of restricting states, which is problematic for the establishment of a secure outer space environment.

IV. Strategic Limitations

If the legal regime is weak on prohibiting ASATs, then why have we not seen a proliferation of those technologies? At the beginning of the space age both the United States and the Soviet Union were keen to explore weapons technologies in the space environment, and both carried out damaging nuclear tests in outer space. However, the results of these tests led these states to establish a strategic restraint in the domain.

During the 1960s, the US and the Soviet Union were racing to develop both military and civil space programs. They both soon saw that these programs had the potential to be incompatible. When the discovery was made that a nuclear explosion in space could destroy satellite that flew through the resulting electromagnetic pulse (EMP), it was recognized that civil and human spaceflight programs would be put at risk by military testing of weapons technology in the space environment. Further, such activities produced risk for passive military uses such as remote sensing for arms control and communication links for military outposts. As a result, in the early 1960s, both nations turned to establishing a regime in which they limited these risks. The Partial Test Ban Treaty and the Outer Space Treaty are the direct results of this effort. While the legal mechanisms that were promulgated in this time period were, as discussed above, weak, the technical reasons for avoiding an outbreak of this technology was strong. This meant that though the law placed no direct prohibition on kinetic ASATs the superpowers refrained in their pursuit of these weapons for a variety of reasons including the risk that they posed to their civil space programs and

human spaceflight. Though both states maintained ASAT development and testing programs into the 1980s, neither developed fully operational systems.
The danger that space debris poses affects every space actor, and in the post-Cold War environment, while there has been limited testing of ASATs, the resulting debris from kinetic ASATs is such that no state has seriously pursued this option. The recent tests that have been conducted by China, the United States, and India can be read as strategic signaling rather than deployment of operational systems. Instead, the more that a state depends on space technology the more that state has to gain from a stable and secure space environment. This, in itself, has been a powerful restraint on the deployment of kinetic ASATs, especially since those states that have the capability in reach are also those states that have a lot to lose.
As the rhetoric surrounding space security heats up, it is important to remember that there are critical environmental reasons for avoiding space debris creation through kinetic ASATs. So while there are three contemporary examples of kinetic ASATs, these states still do not seem to be investing large sums in developing fully operational ASAT systems. This is likely because all three recognize the value of limiting space debris creation events, especially in light of the fact that all three are pursuing commercial gains in the space environment. They want to send a signal that "we can," but do not necessarily want to pursue these technologies to their logical conclusion.

V. OMG ASAT

Cybertechnologies change this strategic math. The simple question that states now face is whether having ASAT capability that does not result in the creation of space debris is destabilizing in the same way that a kinetic ASAT is. The simple answer is "no," especially in light of the fact that a cyber-ASAT has the potential to be unattributable to the state engaging in the attack. In short, a cyber-ASAT capability changes the strategic reasoning that has been critical in dissuading states from pursuing fully operational ASAT capabilities.
Of course, this phenomenon is not limited to the space domain. Cyber-capabilities are changing the ways in which states interact. The ability to reach inside the borders of another state and physically manipulate that environment is powerful. Coupled with the fact that attribution issues mean that tracing the attack back to its origins is difficult, cyber-capabilities are an incredible new tool for states. This tool essentially allows states to sidestep the strictures of the UN Charter's Article 2(4) by operating in grey areas, both technical and legal. While certainly a cyberattack of a certain magnitude will result in a violation of Article 2(4), the ambiguity as to when it reaches this magnitude means that states have enjoyed new freedom of action in the cyber-domain because it changes the way that states understand territorial integrity.

The case of Stuxnet is instructive. In this case, the United States and Israel used a computer virus to cause physical damage at a uranium enrichment facility in Iran. The United States and Israel both denied the attack despite overwhelming evidence that they originated the attack, and Iran never accused them directly of perpetrating the attack. Thus, these states accomplished with a computer, that which would have traditionally required a bomber.

The same can be expected to play out in the space domain, where states might be able to accomplish with computer code that which used to require a missile. However, in the space domain cyber does not just change the assumptions that underly Art. 2(4), cyber undermines the technological realities of space debris that led to strategic restraint. If a state can turn off an adversary's satellite without causing debris, and rely on ambiguity in attribution, then there are numerous strategic reasons to develop this technology rather than strategic restraints.

VI. Conclusion

In short, the future of ASAT is cyber-capabilities. This is not to say that these capabilities are easy or consistently reliable. Indeed, cyber has its own set of limitations that serve to restrain its uses. For example, once a cyber-capability is used, it will be known and easier to defend against in the future. However, any cyber-ASAT capability dramatically changes the traditional legal and strategic restraints on the use of ASATs. Militaries already see the denial of space as a critical need in future warfare. To be able to do so without compromising one's own space infrastructure will mean that the historical limitations on ASAT weapons may melt away leaving the space domain at risk.