FEATURE

Space Pirates, Geosynchronous Guerrillas, and Nonterrestrial Terrorists

Nonstate Threats in Space

Gregory D. Miller, PhD

> *One of the policy implications of the second space age is that the availability of advanced space capabilities on the commercial market can potentially bring the advantages of space within the reach of rogue nations and non-state actors.*
>
> —Todd Harrison, Zack Cooper, Kaitlyn Johnson, and Thomas Roberts
> "Escalation and Deterrence in the Second Space Age"
> *Center for Strategic and International Studies*

President Donald J. Trump's 2017 *National Security Strategy* (*NSS*) posits the return of great-power competition, particularly calling out Russia and China as rivals, and highlights the need to reemphasize space both for defense and commerce.[1] Shortly after the publication of the *NSS*, the president called for the creation of a Space Force, at least partly to defend US security and economic interests in space, and then directed the Pentagon to create a Space Force with his signing of Space Policy Directive-4 on 19 February 2019.[2]

China and Russia continue to develop a range of antispace capabilities, including computer viruses, jamming, lasers, and antisatellite missiles. Yet losing space

superiority to other major powers is a far cry from being targeted in space. Despite the fact that great-power competition will include rivalry in space, space also involves a great deal of cooperation, for example, between the US and Russia, and with the International Space Station.[3] As a result, the most likely scenarios involving attacks against US interests in space may not come from other states. Instead, they involve nonstate actors seeking to challenge the existing international order, overturn the status quo in their countries, or profit from the lack of attention paid to them by the community of nations.

There is danger in focusing too heavily on great-power competition and extending it into space. One potential consequence is the creation of a self-fulfilling prophecy through the security dilemma; by emphasizing the probability of conflict between great powers, and by enhancing military capabilities to address potential threats, a state actually increases the likelihood of conflict.[4] A second problem is that focusing too much on states ignores the potential threat of nonstate actors who may be harder to deter because they have less fear of reprisal, are less concerned about escalation to war, and have less to lose by targeting space assets. Adam Routh suggests that as the commercial space sector grows and provides more value to the global economy, "this growth will increase the cost to those who wish to attack space systems." But that growth focuses on the second-order consequences of states attacking in space and ignores those nonstate actors who do not care about the world's economy or would relish the ability to weaken the global economic system.[5]

This article examines the nature of the threat from nonstate actors. Although the impetus for the article is the potential rise of a US Space Force, the ideas expressed here are applicable to all states with interests in space. It focuses on three types of nonstate actors: two with political motivations (guerrillas and terrorists) and one with mostly economic motivations (pirates). It derives its ideas from scholarly work and historical examples of how these actors traditionally behaved toward states, then extrapolates to potential activities against space assets.

The article is divided into three sections. First, it examines two different types of political actors: guerrillas and terrorists. It discusses the differences between the terms, examines how those differences are relevant to the space domain, and then uses their historical behavior to forecast how they might act against space assets in the future. The article then examines one type of commercial actor, pirates, specifically focusing on their motivations and potential types of activities. The article concludes with some recommendations for states to prepare for their eventual rise and the threat they pose and to deter these types of attacks.

One assumption this article makes is that there will be no direct great-power confrontations in space, at least in the near future. Despite the US's renewed em-

phasis on great-power competition, this article assumes they will deter each other from initiating conflict in space for fear of escalation. While a war could escalate into the space domain,[6] it is flawed to assume that as more states are active in space, they are more likely to have conflict. More states have nuclear weapons today than they did in the 1950s, but a war between the nuclear powers is no more likely today than in the past. For now, the most likely threat of attacks against the space capabilities of any country will come from nonstate actors engaging in new forms of asymmetric warfare. The exact nature and purpose of the attacks will depend on the actor and their goals, which is a heavy emphasis of the sections below.

A second assumption is that the primary threat involving space and nonstate actors will be attacks directed from Earth against the space capabilities of states, rather than attacks that emanate from space. It is still difficult and expensive to place an object in orbit—only a handful of states have that ability[7]—so it will be a while before nonstate actors with violent intentions could weaponize space. However, nonstate actors will develop space capabilities at some point in the near future, even if those capabilities involve simply degrading satellites or stealing communication signals. The ability of western companies (Rocket Lab, Virgin Galactic, and so forth) to develop space capabilities of some type shows that nonstate actors can access space with minimal assistance or funding from states. SpaceX alone plans to deploy thousands of broadband satellites (Starlink) and requested approval for one million earth-based ground transmitters.[8] Not only does this illustrate the growing capabilities of nonstate actors, but it also highlights the number of potential vulnerable targets that are already accessible by nonstate actors.

As states become more reliant on space and as the cost of participating in space declines, it would be overly optimistic to believe that nonstate actors will not become increasingly greater threats, not to mention that nonstate actors can already carry out attacks on the ground that would have negative consequences for a state's interests in space, such as targeting launch facilities or personnel.[9] To prepare for some of these potential challenges, it is important to understand the nature of the actors that may present a threat.

Political Actors

Two types of violent political actors who may have an interest in attacking a country's space assets are guerrillas and terrorists. The differences between these two groups are often perceived to be academic and are biased by one's perspective of a conflict. But understanding the difference is important for decision makers because they relate to the behavior of the group, the degree to which the group has popular support, and how a group will respond to different types of government actions.

One of the most important distinctions between the two types of actors is that guerrillas generally attack military and government targets while terrorists generally attack civilian targets. Because of this distinction, guerrillas see the population as their support base that must be educated to the cause and won over while terrorists see the population as a means to an end that the group must target to achieve its goals. Mao Tse-tung, and later revolutionaries who followed his model, saw guerrilla warfare as part of the second phase of a revolution, the first phase being organization and the third phase being a conventional war.[10] Thomas Marks suggests that violence was a part of every phase of Mao's revolution, and interpreting violence (both terrorism and guerrilla warfare) as only part of the second phase is a misreading of Mao that is common among DOD counterinsurgency documents.[11]

For Mao, the type of violence a group uses is a function of the capabilities of the group relative to those of the state and the level of support the group receives from the local population. This means that whether a group targets civilians or military forces will depend on its capabilities, though Mao also saw the risk of targeting civilian populations and then having to rely on that base for support.

According to David Galula, there are two approaches to an insurgency, each involving five phases, though only the first two phases differ, while the last three phases are the same in each approach. In one approach, which he typically ascribes to revolutionary movements, the first two phases are about building the organization, educating the masses, and establishing a base of support from the population. The third phase then adopts violence in the form of guerrilla warfare. In an alternative process, which Galula relates primarily to nationalist movements, the first two phases use violence to educate, mobilize and build the organization. The first phase uses random acts of terrorism to garner attention to the cause. The second phase involves more selective terrorism to weaken the regime and strengthen the group before the group advances into the third phase of guerrilla warfare.[12]

In addition to the distinction between targeting civilians and combatants, guerrilla forces are generally larger organizations while a terrorist group may include just a handful of individuals. This distinction affects their behavior in several important ways. Guerrillas generally want to hold and keep territory to gain autonomy or independence from their existing government or to take over the government at some point in the revolution. Terrorists usually prefer to avoid holding territory or are not large and powerful enough to do so. Also, guerrillas are more likely to use conventional military tactics and are organized in a hierarchical way, much like a conventional military organization. Terrorists are more likely to use unconventional types of attacks and are more often organized as cells or in ac-

cordance with the concept of leaderless resistance, in which small cells operate autonomously with few connections across cells or between a cell and the larger organization's leaders.[13]

These structural differences further influence the behavior of groups and their vulnerability to government activities.[14] Hierarchical organizations are much more likely to follow the vision of the leader and engage in activities that more obviously reflect the strategic goals of the group. For this reason, guerrilla and terrorist leaders who want personal power, especially those who want to remain in power after achieving success, are more likely to create groups with this type of organization. There are two negatives to this structure: it is easier for strangers to join as new members, and it is easier for one member to gain a great deal of information about the workings of the organization. As a result, it is easier for government agents to infiltrate the organization and thus potentially to defeat it.

Groups with leaderless or cellular structures are more difficult to infiltrate and defeat because new recruits are usually someone known to existing members of the cell. Also, since there are no links between cells, members are unable to identify those in other cells or even the leadership. It is also more difficult to predict the behavior of leaderless groups because they do not answer to a single leader or follow one person's strategic vision. Cells within the organization may even engage in behavior that is rational for themselves but contrary to the interests of the movement as a whole, making it more difficult for a leader to control the organization. As a result, deterrence is more challenging against leaderless organizations.[15]

Despite these differences, the organizations themselves often muddle the distinction between guerrilla warfare and terrorism by engaging in both types of activities. In contrast to the concept of discreet phases, groups that are generally guerrillas sometimes attack civilians, and terrorist groups sometimes attack military targets. The distinctions will likely become even blurrier in space with many satellites having dual-uses, involving both military and civilian capabilities. Attacks against the Global Positioning System (GPS) constellation, for instance, could be targeting the US military or US society, or even nonstate actors dependent on the GPS system. Only the intent of the attack would help determine whether it would be considered guerrilla warfare (attacking military targets) or terrorism (attacking noncombatants), though that would only happen after the identification of the perpetrator, at which point that would be a mostly academic distinction. The result would be the same for the US government and the millions of people and businesses that rely on GPS.

Even if the differences between the groups were clear, should we consider personnel in space to be civilians or military? US astronauts who come from the military typically remain on active duty while seconded to the National Aeronau-

tics and Space Administration (NASA). Others who serve as scientists, engineers, and medical professionals, for example, are civilian federal employees. Also, not even the military officers would qualify as combatants while engaged in a space flight since they are not armed, nor are they in a combat zone.[16] Unless engaged in offensive space operations, most astronauts are noncombatants. As a result, attacks against them would be terrorism rather than guerrilla warfare (or war crimes if perpetrated by a state).

Having discussed some of the similarities and differences between the two types of actors, let us now turn to their likely activities. The distinction between guerrilla and terrorist will not fully determine their behavior as much as their purpose will, but the purpose often indicates which types of attacks a group will use and so contributes to whether a group is labeled guerrilla or terrorist. Important distinctions within each category may also influence a group's behavior.

Guerrillas are often domestic groups targeting their own government with the goal of establishing an independent state, or they are engaged in a struggle against a foreign power that they view as an occupying force.[17] Historically, many of these types of groups were motivated by a revolutionary cause (the Marxist-Leninist ideology of the Revolutionary Armed Forces of Colombia, as an example, or the Maoist ideology of Peru's Shining Path), where they sought a dramatic change in society and the government. Others are motivated by a desire for independence (like the Liberation Tigers of Tamil Eelam (LTTE) in Sri Lanka).[18] They may receive aid or support from outside parties, which can include financial, ideological, and military support and even personnel, but they typically have local rather than global goals. As a result, attacks in space by guerrillas would likely target their own government's capabilities or states that appear to be meddling in their national affairs. One example was the insurgency's use of jamming during Operation Iraqi Freedom. According to the "Space Threat Assessment 2018," insurgents deliberately jammed commercial satellite communications links used by the US military.[19] As long as those actors stuck to purely military targets, they would remain—at least in an academic sense—guerrillas.

Because most guerrillas would like the international community to view them as having legitimacy, and they would like to govern themselves at some point, either as a separate state or in a newly reconstituted state, they often refrain from attacks that are potentially costly to the civilian population, though there are exceptions where guerrilla groups engaged in terrorist activities. Also, guerrillas often value the sympathy or support of other states and of the international community. As a result, it is unlikely that groups that fall closer to the guerrilla side of the spectrum will engage in attacks against space interests that have long-term and broader consequences. For instance, these groups are unlikely to use kinetic

weapons to attack space assets. Such attacks would create a debris field that could subsequently damage other states' assets and potentially hurt or inconvenience civilian populations. Such consequences would weaken international support and so guerrilla groups will likely refrain from such activities. That does not mean kinetic attacks will not happen, just that they are more likely to be the work of terrorists who are less concerned with international perceptions. Instead, attacks by guerrillas are more likely to focus on effects like degrading an orbit, disabling a capability (like a state's communications satellites), or blinding a surveillance satellite to reduce a state's military advantage when engaging with the guerrilla forces.

Because of the similarities between space and cyberspace, we should also expect groups to engage in multidomain attacks using any available new technologies. As early as 1999, hackers seized control of a British military communications satellite with a home computer.[20] Guerrilla groups historically engage in a variety of cyber attacks, mostly to harass governments or to deny service to government agencies. For example, the LTTE, the now-inactive Tamil insurgent group in Sri Lanka referenced earlier, often engaged the Sri Lankan military in guerrilla warfare but also carried out terrorist attacks. It had a cyber unit as early as 1997 that frequently targeted the government. Beyond using its own website for propaganda and financing, the LTTE hacked government networks, engaged in denial of service attacks, and engaged in propaganda and counterpropaganda by hacking websites. In 2007, they even pirated a US satellite to send broadcasts to other countries.[21] Similar types of attacks are likely to occur against space assets as more groups gain the capability to do so.

Terrorist attacks against space capabilities could come in a variety of forms based on numerous motivations. Terrorist motivations could be driven by nationalism or a revolutionary ideology, similar to what motivates guerrillas but targeting civilians to achieve the group's goals. Groups also use terrorism for a variety of other reasons that may be local, regional, or global. Examples include religious differences, for antitechnological purposes, or simply as part of a neoanarchist movement hoping to prevent governments from becoming even more powerful through the exploitation of space.

Terrorists engage in several different types of tactics, against a variety of targets, though the target is often linked to the broader goals of the group. For instance, Marxist groups are more likely than others to target private businesses, religious groups are more likely than other types of groups to target other religions, and white supremacist groups often attack minorities or minority businesses. Given that terrorists—and guerrillas, for that matter—generally attack targets that are consistent with their strategic goals, what would motivate groups to target a country's space assets? It could simply be a group that wants to reduce the power of the

state or a group that opposes the state's ideology. Also possible are attacks by groups that oppose the weaponization of space or that oppose technology more broadly, focusing on a state's policies in space rather than the nature of the state itself, much as single-issue terrorists focus on a state's treatment of animals or its abortion laws. Many Americans oppose spending money on space when there are economic or social problems at home, so it is not too much of a stretch to expect violence in opposition to using resources on space.[22]

Terrorists are generally less concerned with political backlash than are guerrillas. They are less likely than guerrillas to worry about the ramifications of creating debris in space or of inconveniencing civilian populations. That means terrorists are more likely to employ some type of kinetic capability, such as antisatellite rockets. This is consistent with the record of terrorist activity on the ground, which overwhelmingly involves the use of bombs or explosives. According to the Global Terrorism Database, bombings account for 49 percent of all terrorist activity between 1970–2017. For comparison, the next most common tactics are armed assaults and assassinations, accounting for 25 percent and 11 percent, respectively, though there is some temporal and regional variation.[23]

Also, while terrorists often attack targets related to their goals, they sometimes attack symbolic targets or targets intended to elicit a reaction (usually an overreaction from a government).[24] The al-Qaeda attack on 9/11 was as much for symbolic value and to get a US response as it was to achieve a group objective. As a result, we cannot rule out the possibility of a terrorist group attacking a state's space interests to generate publicity or to show it has the ability to attack a target even in space.

Having said that, such a capability will be difficult for independent groups to achieve in the near-term. Because terrorists are generally less capable than guerrillas, those who are capable of attacking space interests will most likely be either larger organizations with the ability to develop applicable resources, and/or groups that have a state or corporate sponsor that provides those capabilities. While the most likely source may be a state sponsor, states are also more likely to reign in their proxy groups to avoid retaliation from the target. As long as only a small number of states could carry out an attack in space, states will be reluctant to furnish terrorist groups with those capabilities, out of fear of easy attribution and retaliation.

On the other hand, as the number of actors with such capabilities grows, attribution will become more difficult, and states may accept the risk of allowing a proxy to carry out an attack if it weakens an adversary's ability to wage war or defend its interests. And as the cost of entry comes down, more groups will have the ability to carry out attacks. Even smaller independent groups now have the

ability to carry out conventional attacks against launch facilities on the ground and personnel affiliated with space. According to a 2008 briefing by Randy Jones, director of the Defense Intelligence Agency's Missile and Space Intelligence Center, terrorists already had the ability to engage in cyberattacks and the jamming of satellites and could disable satellites with lasers by 2020.[25]

There are several other ways groups could target a state's space assets. Once a group has the ability to put something in orbit, it could self-detonate and the debris field itself would threaten any assets in that orbit. Authorities are particularly concerned about nonstate actors being able to use our own technology against us. One fear is of satellite systems being used for microwave-like attacks. Another is the targeting of the atomic clocks on GPS satellites, which could effectively "warp time."[26] Given there are already private companies capable of launching objects into orbit, we should not assume these are simply theoretical scenarios.

Although it may seem unlikely terrorist groups would target space capabilities, it is not without historical precedent. As far back as 1972, groups were thinking about using attacks against space assets to enhance their cause or gain more publicity. The Black September Palestinian group threatened an attack against the Apollo 17 mission, specifically to murder or kidnap the crew or their families. That same group killed Israeli athletes at the Munich Olympic Games earlier that year, so NASA took the threats seriously.[27] Joshua Gelernter claims the attacks were thwarted, while Eugene Cernan's autobiography suggests security patrols were added to the families' homes and schools, but no attack took place.[28] More recently, in 2003, NASA increased security for the Columbia shuttle launch, out of concern that al-Qaeda would attack the launch pad because of the Israeli astronaut on the flight.[29] In 2013, a letter threatening terror attacks was found at an Indian Space Research Organization (ISRO) facility in Bangalore, India.[30]

It is one thing to threaten an attack, or for an agency to be concerned about attacks, but there have been real attacks against ground installations and satellites. On 3 August 1984, just two days before the launch of an Ariane satellite, the French left-wing group Action Directe bombed the European Space Agency's (ESA) Paris headquarters, injuring six people.[31] The ESA was also hacked in 2015 by the group Anonymous, resulting in the leak of thousands of credentials.[32] Also, an ISRO computer was infected with malware, which could have given hackers control of rocket launches and satellite separation.[33] While violent extremist organizations are not responsible for these last two attacks against ESA and ISRO, the incidents illustrate the existing capabilities of nonstate actors.

Also, if states continue to use their space capabilities to target nonstate actors, then we should expect space assets to become a bigger target for these groups. As an example, the Indian government used its satellites to help strike terrorist camps

in Kashmir.[34] Such uses of technology are valuable but also invite retaliation against the technology itself, or its operators.

One tactic used by modern terrorists is suicide bombings.[35] While this type of attack is often associated with Islamic extremist groups, not all Islamic groups engage in the tactic and other types of groups use suicide bombings. The most prominent non-religious group to use suicide bombing is the now-inactive LTTE, discussed above. There is significantly less history of suicide bombings being carried out by either right-wing or left-wing groups, or by single-issue groups (groups engaged in violence over a specific interest like animal rights, environmental rights, antiabortion, and so forth). Because of the difficulty of putting people in space for the near term, terrorists are unlikely to use this tactic against assets in space, though it may still be used by certain types of terrorist groups—presumably those already inclined to the use the tactic—against ground facilities and personnel.

While the distinction between terrorists and guerrillas often seems academic, the difference is real and important because it is based on the activities of the group, and that affects the degree to which any particular group poses a threat to a state's interests in space. While the distinction is important, just as important is the group's motivation for carrying out violent attacks in the first place, regardless of whether they are directed at civilians or military, on the ground or in space. The conclusion discusses some of the ways these groups respond differently to state actions and proposes measures to both deter and defend against actors motivated by political goals, particularly when compared to those motivated by commercial interests.

Commercial Actors

Although we cannot rule out the possibility of companies engaging in a variety of activities against competitors, including corporate espionage, theft of intellectual property, and sabotage, the most likely near-term scenarios involve what is more accurately thought of as piracy. In these scenarios, nonstate actors, operating either on their own or under the direction of a company or state, will engage in violent activities against a state's interests in space. These attacks are less likely to be about causing mayhem or achieving some political goal and are more likely to involve the types of activities that can generate a profit for the group or garner market advantages for its sponsor. From October 2010–September 2011, NASA computers experienced more than 5,400 incidents of malicious software or unauthorized access, in some cases described as having "full control over those networks." Some of these, according to investigations, may have come from individual hackers and some from foreign intelligence services, but others were carried out by criminal groups attempting to profit off the information they obtained.[36]

Unlike guerrilla warfare and terrorism, where there is neither a consensus academic definition nor an accepted definition in international law, there is a United Nations definition of *piracy*. Article 101 of the United Nations Convention on the Law of the Sea (UNCLOS), adopted in 1982 and currently ratified by 167 states, defines piracy as:

> (a) any illegal acts of violence or detention, or any act of depredation, committed for private ends by the crew or the passengers of a private ship or a private aircraft, and directed:
>
> (1) on the high seas, against another ship or aircraft, or against persons or property on board such ship or aircraft;
>
> (2) against a ship, aircraft, persons or property in a place outside the jurisdiction of any State[37]

This definition is an appropriate starting point for attacks by nonstate actors in space, given the lack of state jurisdiction, and because it includes attacks against property and not just people.[38] There are two interesting elements of the UNCLOS definition when applied to *space piracy*. One is that it obviously focuses on maritime piracy but ignores broader acts of theft that one could also describe as piracy. These acts can involve the theft of intellectual property, theft of communication signals and the information they contain, or even the theft of property itself.[39] The second interesting element of the UNCLOS definition is the phrase "for private ends," which is somewhat broad, but which I interpret to mean for profit or for commercial gain. This sets apart nonstate actors who engage in piracy from the guerrillas and terrorists who engage in violent activities for political gain.

If nonstate actors believe it is possible to profit from any of these activities, then we will see space pirates emerge. Three likely sources of revenue from this type of activity include groups: 1) operating on their own and selling what they steal (most likely information); 2) acting as a proxy for a company targeting its competitors (most likely involving sabotage or corporate espionage); or 3) having a state sponsor that provides financial support in exchange for sowing disorder on an adversary. While this third source of funding blurs the line between commercial and political activities, if the group does not itself have political goals in attacking targets, then it is acting purely for private, mercenary ends and is a commercial actor.[40]

Groups operating off the coasts of Somalia and western Africa are perhaps the best illustrations of modern-day maritime piracy. These groups may have some political goals in terms of controlling their local territory (that is gaining or preserving power), but their activities against commercial shipping are primarily for profit and even their territorial goals are ultimately about financial security. In

most cases, these groups seize a ship and its cargo and eventually release crewmembers. Although pirates have killed some crewmembers, most would rather receive a ransom for the release of the crew. North Atlantic Treaty Organization and European Union operations against piracy have been relatively effective,[41] and this provides one possible model for dealing with space piracy. One state acting alone cannot resolve the problem, because threats to commerce affect the international community, and actors engaged in that behavior will need to be dealt with collectively. Nor do current counterpiracy operations adequately address the root causes of piracy, which often involve a breakdown of local government. Likewise, current international law is not set up adequately to address the problem of space piracy.[42]

On the other hand, recent cyberattacks suggest that states that are the target of attacks by a company or state using a nonstate proxy will be left to deal with the attack largely on their own.[43] That does not mean international cooperation cannot work under such circumstances, just that it is less likely when multiple interests are not being threatened. It does mean states need to be thinking about the ramifications of similar behavior in space, and whether current laws and treaties sufficiently address the problem. One reason the US has not ratified UNCLOS is concern over the potential precedent it might set for space.[44] But that may be the best reason for the US to ratify UNCLOS now because it would provide states greater flexibility and leverage to go after nonstate actors responsible for carrying out attacks in space.

Conclusions and Recommendations

This article is a preliminary examination of the possible threats to states from nonstate actors. It cannot possibly cover all the scenarios that threaten space capabilities or utilize space to threaten states themselves. It is intended as a starting point to spur thinking about the reality that future conflicts will not involve just great powers, as much as the DOD might be more comfortable preparing for peer competition and distancing itself from the types of operations it employed in the last decade and a half. A 2016 Chatham House research paper suggested that, along with nation-states and individual hackers, "cyberthreats against space-based systems include... well-resourced organized criminal elements seeking financial gain; [and] terrorist groups wishing to promote their causes, even up to the catastrophic level of cascading satellite collisions."[45] States clearly pose the greatest threat to space assets if we only focus on capabilities. The more likely threat comes from nonstate actors. If we stop thinking about asymmetric warfare or the ability of nonstate actors to influence states, then states will be caught off-guard by at-

tacks that should otherwise be anticipated. This is as true in the space domain as it is on the ground.

Unfortunately, current technology makes space an offense-dominant domain. Despite the cost and technological difficulty of reaching space, it is relatively easy to carry out attacks, at least compared to the cost of defending capabilities in space. As the cost of entry declines over time, if offense remains dominant, then the application of asymmetric space warfare by nonstate actors will become an even greater threat to all states with interests in space. A critical question moving forward is whether the space domain, by its nature, will perpetually favor the offense or if defense will eventually become prominent. The history of warfare suggests that when offense has the advantage, governments will pursue more effective defenses, to overcome an adversary's offensive advantages. As a result, one thing states must do is pursue defensive capabilities in space, both to defend against attacks from nonstate actors and to reduce the likelihood of war.[46] Violence between states become less likely when leaders believe it is easier to defend than to attack, so while it can be difficult to distinguish between offensive and defensive capabilities, enhancing the defensive capabilities of all space assets will reduce the threat of nonstate actors without decreasing stability in the international system.[47]

Where that distinction between *terrorist* and *guerrilla* might matter most is in how states deal with those who carry out such attacks, though states traditionally deal with domestic actors the same way regardless of their label and nationality.[48] The fact that space is not sovereign territory for any one country would further complicate things because it would necessarily involve international law. Although attacks may target people on the ground, most attacks in space would be directed against property, posing a challenge for states that want to identify such attacks as terrorism. The Federal Bureau of Investigation definition of *terrorism* includes attacks against property,[49] and although the DOD definition leaves room for attacks against property, it does not specifically reference such attacks as being acts of terrorism.[50] As a result, attacks by nonstate actors against a civilian asset in space, might not be considered an act of terrorism by the DOD but would be terrorism by the FBI as long as it satisfied the other elements of the definition. These issues are beyond the scope of this article, but the broader point is that many states still struggle with how to deal with nonstate actors who engage in political violence on the ground. This will be further complicated when non-state actors begin to target state capabilities in space.

Beyond emphasizing defensive measures, to what extent can states deter any of these nonstate actors from engaging in attacks against space interests? All three types of actors discussed in this article—pirates, guerrillas, and terrorists—are generally rational, so by traditional deterrence logic they should be deterrable.

However, selfish actors are deterred more easily than those who are acting for selfless reasons,[51] so pirates should be more easily deterred than either guerrillas or terrorists since pirates are pursuing a financial gain that directly benefits them, rather than a political goal that might only benefit future generations. That does not mean deterrence will not work against groups with political motivations, but the same challenges for deterring terrorist groups on the ground apply to deterring their activities in space. According to the CSIS Space Threat Assessment 2018, "Deterrence can be particularly challenging for non-kinetic, electronic, and cyber methods of attack because these can be more difficult to detect and attribute and can have reversible effects."[52] States will have to be clear what activities they wish to deter, increase their ability to assign attribution to specific actors, and then have the ability and will to respond if actors ignore their deterrent threats. At the same time, states have to be cautious of overreaction, because terrorists often attack to elicit an extreme response from a government, which further increases awareness of the group's cause or sympathy for the group itself.

In the case of state or corporate sponsors, states will also have to make deterrent threats against them and must again have the ability and will to punish those sponsors for the activities of their proxies. Also, maintaining the support of international partners and various populations will be critical and perhaps limit the ability of states to respond using military force, but the other instruments of national power (diplomatic, informational, and economic) may be more effective against these groups and their sponsors. This means understanding the reasons a group might engage in violence and addressing any legitimate complaints that lead people to join that group to reduce the number of sympathizers in the population and shrink the possible base of support.

Beyond developing the defensive capabilities to reduce the effects of an attack, and enhancing attempts to deter nonstate actors, how will we treat captured pirates, guerrillas, and terrorists? The answer is complicated by the nature and location of the attack, the citizenship of the responsible actors, and who captures them and where. The jurisdiction would likely be that of the international community since national sovereignty does not extend into space. Yet even that is more complicated because states own their space assets. As with cyberattacks that could emanate from anywhere, an attack against a US satellite would likely fall under US jurisdiction to prosecute, assuming the responsible parties could be arrested and extradited to US soil. In the end, states and the international community need to expand discussions dealing with nonstate threats to space because such responses will necessarily rely on a mix of individual state laws, international law, and international norms. Hopefully, this article pushes leaders toward thinking in those terms and avoiding a tunnel-vision focus on great-power competition. ✪

Notes

1. However, the *National Security Strategy* does not refer to these rivalries as hostile. Executive Office of the President of the United States, *National Security Strategy of the United States of America* (Washington, DC: US Government Printing Office, December 2017), https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

2. In a statement at the beginning of the third meeting of the revived National Space Council, President Trump said, "I'm hereby directing the Department of Defense and the Pentagon to immediately begin the process necessary to establish a Space Force as the sixth branch of the armed forces." Sandra Erwin, "Trump: 'We Are Going to Have the Space Force,'" *Space News*, 18 June 2018, https://spacenews.com/trump-we-are-going-to-have-the-space-force/; and Mike Wall, "Trump Signs Directive to Create a Military Space Force," *Space.com*, 21 February 2019, https://www.space.com/president-trump-space-force-directive.html.

3. Hanna Krueger, "In Space, U.S. and Russia Friendship Untethered," *NBC News*, 30 September 2017, https://www.nbcnews.com/news/us-news/space-u-s-russia-friendship-untethered-n806101; and Simon Saradzhyan and William Tobey, "US-Russian Space Cooperation: A Model for Nuclear Security," *Bulletin of the Atomic Scientists*, 7 March 2017, https://thebulletin.org/2017/03/us-russian-space-cooperation-a-model-for-nuclear-security/.

4. Robert Jervis, "Cooperation under the Security Dilemma," *World Politics* 30, no. 2 (January 1978): 167–214, https://www.jstor.org/stable/2009958?seq=1#page_scan_tab_contents; and Charles Glaser, "The Security Dilemma Revisited," *World Politics* 50, no. 1 (October 1997): 171–201, https://www.jstor.org/stable/25054031?seq=1#page_scan_tab_contents.

5. Adam Routh, "The U.S. Military Should be Doubling Down on Space," *DefenseOne.com*, 1 August 2018, https://www.cnas.org/publications/commentary/the-u-s-military-should-be-doubling-down-on-space.

6. Gen John W. "Jay" Raymond, head of US Air Force Space Command stated: "Space is a warfighting domain just like air, land and sea. We have to be prepared to fight a full range of operations." Quoted in Colin Clark, "Exclusive: War in Space 'Not a Fight Anybody Wins'—Gen. Raymond," *Breaking Defense*, 6 April 2017, https://breakingdefense.com/2017/04/exclusive-war-in-space-not-a-fight-anybody-wins-gen-raymond/.

7. As of 2018, 72 governments had a space agency. Of those, 14 had proven orbital launch capabilities, only three of which have put a human into space (India hopes to be number four by 2022). Peter Farquhar, "Australia Finally has a Space Agency—Here's Why It's about Time," *Business Insider Australia*, 2 July 2018, https://www.businessinsider.com.au/australia-space-agency-value-2018-7; and Swati Gupta, "On Independence Day, Modi Promises Manned Space Mission," *CNN*, 15 August 2018, https://www.cnn.com/2018/08/15/asia/india-manned-space-flight-intl/index.html.

8. Arthur Villasanta, "SpaceX to Build 1 Million Earth Stations to Track 12,000 Satellites, FCC License Details," *International Business Times*, 10 February 2019, https://www.ibtimes.com/spacex-build-1-million-earth-stations-track-12000-satellites-fcc-license-details-2761987.

9. In 2004, Russian military security forces placed the Baikonur Cosmodrome on the top of its list of potential terrorist targets in Kazakhstan. James Oberg, "Earthly Threats for a Spaceport: Baikonur Faces Future Insecurity Without Military Presence," *Space Review*, 26 June 2006, http://www.thespacereview.com/article/647/1/. After 9/11, the US became particularly concerned with security involving the shuttle program, as well as how to use the space program in the War on Terror. Also, *see* Denise Chow, "NASA & Military After 9/11: Grappling with US Space Security," *Space.com*, 8 September 2011, https://www.space.com/12867-september-11-nasa-military-space-security.html.

10. Mao Tse-Tung, *On Guerrilla Warfare* (Champaign, IL: University of Illinois Press, 2000).

11. Marks cites Joint Publication 3-24, *Counterinsurgency Operations*, as one example. *See* Thomas Marks, "Mao Tse-tung and the Search for 21st Century Counterinsurgency," *CTC Sentinel* 2, no. 10 (October 2009): 17–20, https://ctc.usma.edu/mao-tse-tung-and-the-search-for-21st-century-counterinsurgency/.

12. David Galula, *Counterinsurgency Warfare: Theory and Practice* (Westport, CT: Praeger Security International, 1964), 30–42.

13. Louis Beam, a white supremacist leader, wrote one of the earliest works on this model. Beam, "Leaderless Resistance," *The Seditionist*, 12 February 1992, http://www-personal.umich.edu/~satran/PoliSci%2006/Wk%2011-1%20Terrorism%20Networks%20leaderless-resistance.pdf.

14. Several authors examine how a group's organizational structure influences its behavior. For example, Victor Asal and Karl Rethemeyer, "The Nature of the Beast: Organizational Structures and the Lethality of Terrorist Attacks," *Journal of Politics* 70, no. 2 (April 2008): 437–49, https://www.jstor.org/stable/10.1017/s0022381608080419?seq=1#page_scan_tab_contents; and Baoz Ganor, "Terrorist Organization Typologies and the Probability of a Boomerang Effect," *Studies in Conflict & Terrorism* 31, no. 4 (April 2008): 269–83, https://www.tandfonline.com/doi/abs/10.1080/10576100801925208?tab=permissions&scroll=top/.

15. Gregory D. Miller, "Terrorist Decision Making and the Deterrence Problem," *Studies in Conflict & Terrorism* 36, no. 2 (February 2013): 132–51, doi: 10.1080/1057610X.2013.747075/.

16. Noncombatants include civilians, as well as military personnel (whether or not armed or on duty) who are not deployed in a war zone or a war-like setting. 22 USC 2656f(d)(2) as interpreted by US Department of State, *Country Reports on Terrorism 2017* (September 2018), 339.

17. The DOD definition of a guerrilla force is: "a group of irregular, predominantly indigenous personnel organized along military lines to conduct military and paramilitary operations in enemy-held, hostile, or denied territory." Joint Staff, *Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms* (15 February 2016), s.v. "guerrilla force," https://fas.org/irp/doddir/dod/jp1_02.pdf.

18. Some independence movements also had Marxist-Leninist motives during the Cold War although many have since moderated their ideological motivations to focus on independent governance.

19. Todd Harrison, Kaitlyn Johnson, and Thomas Roberts, "Space Threat Assessment 2018," *Center for Strategic & International Studies*, April 2018, 24, https://aerospace.csis.org/wp-content/uploads/2018/04/Harrison_SpaceThreatAssessment_FULL_WEB.pdf.

20. "Satellite Hack Raises Security Questions," *CNET*, 2 January 2002, https://www.cnet.com/news/satellite-hack-raises-security-questions/.

21. John Daly, "LTTE: Technologically Innovative Rebels," *Asian Tribune*, 14 June 2007, http://www.asiantribune.com/; and Peter B. de Selding, "Intelsat Vows to Stop Piracy by Sri Lanka Separatist Group," *Space News*, 18 April 2007, https://spacenews.com/intelsat-vows-stop-piracy-sri-lanka-separatist-group/.

22. Alexis C. Madrigal, "Moondoggle: The Forgotten Opposition to the Apollo Program," *Atlantic*, 12 September 2012, https://www.theatlantic.com/technology/archive/2012/09/moondoggle-the-forgotten-opposition-to-the-apollo-program/262254/.

23. National Consortium for the Study of Terrorism and Responses to Terrorism, 2018, Global Terrorism Database (data file), retrieved from https://www.start.umd.edu/gtd.

24. Bruce Hoffman, "Aviation Security and Terrorism: An Analysis of the Potential Threat to Air Cargo Integrators," *Terrorism and Political Violence* 10, no. 3 (1998): 54–69, https://www.tandfonline.com/doi/abs/10.1080/09546559808427469?src=recsys; and Mohammed Hafez, "Dying to Be Martyrs: The Symbolic Dimension of Suicide Terrorism," 54–80 in Ami Pedahzur, ed., *Root Causes of Suicide Terrorism: The Globalization of Martyrdom* (London: Routledge, 2006).

25. Noah Shachtman, "Pentagon Spy: Terrorists Ready to Launch Satellite Strikes by 2020," *Wired*, 25 June 2008, ttps://www.wired.com/2008/06/the-defense-int/. While some of this assessment may have been overly pessimistic, it does highlight the options available to nonstate actors more than a decade ago.

26. Alex Hern, "Hacked Satellite Systems Could Launch Microwave-Like Attacks, Expert Warns," *The Guardian*, 9 August 2018, https://www.theguardian.com/technology/news-blog/2018/aug/09/satellite-system-hacking-attacks-ships-planes-military; and Molly McCrea and Joe Vazquez, "Experts Warn GPS Vulnerable to Time-Tampering Terrorism," *KPIX*, 1 November 2018, https://sanfrancisco.cbslocal.com/2018/11/01/gps-satellites-vulnerable-terrorism-hackers/.

27. David Schlom, "Target America 1972: When Terrorists Threatened Apollo," *Ad Astra* 13, no. 6 (November–December 2001): 20–24, https://space.nss.org/ad-astra-volume-13-number-6-2001/.

28. Joshua Gelernter, "Remembering Gene Cernan," *Weekly Standard*, 23 January 2017, https://www.weeklystandard.com/joshua-gelernter/remembering-gene-cernan; and Eugene Cernan and Don Davis, *The Last Man on the Moon: Astronaut Eugene Cernan and America's Race in Space* (New York, NY: St. Martin's Press, 1999), 284–85.

29. Jeff Stein, "NASA Worried about al-Qaeda Attack on Shuttle," *Washington Post*, 18 June 2010, http://voices.washingtonpost.com/spy-talk/2010/06/white_house_worried_about_qaed.html.

30. "Police Step up Vigil after Terror Threat to ISRO, HAL," *Economic Times*, 20 June 2013, https://economictimes.indiatimes.com/news/politics-and-nation/police-step-up-vigil-after-terror-threat-to-isro-hal/articleshow/20684149.cms/.

31. Associated Press, "Bomb Shatters Office Of Europe Space Unit," *New York Times*, 3 August 1984, https://www.nytimes.com/1984/08/03/world/bomb-shatters-officeof-europe-space-unit.html.

32. Darlene Storm, "Attackers Hack European Space Agency, Leak Thousands of Credentials 'for the Lulz'," *Computerworld*, 14 December 2015, https://www.computerworld.com/article/3014539/attackers-hack-european-space-agency-leak-thousands-of-credentials-for-the-lulz.html.

33. Mithun MK, "ISRO Computer Had Malware, Could've Been Hacked, Say Researchers," *New Indian Express*, 12 March 2018, http://www.newindianexpress.com/cities/hyderabad/2018/mar/12/isro-computer-had-malware-couldve-been-hacked-say-researchers-1785758.html.

34. Vidya Sagar Reddy, "ISRO's Commitment to India's National Security," *Space Review*, 31 October 2016, http://www.thespacereview.com/article/3092/1.

35. Since 1981, suicide attacks account for less than 4 percent of all terrorism, though that was at 6 percent between 2007–17, and almost 7.5 percent during 2016–17. Also, suicide terrorism accounts for more than 10 percent of all fatalities from terrorism. Global Terrorism Database (Data file), retrieved from https://www.start.umd.edu/gtd/.

36. Emil Protalinski, "NASA: Hackers Had 'Full Functional Control'," *ZDNet*, 2 March 2012, https://www.zdnet.com/article/nasa-hackers-had-full-functional-control/.

37. United Nations Convention on the Law of the Seas, 10 December 1982, http://www.un.org/Depts/los/convention_agreements/texts/unclos/UNCLOS-TOC.htm.

38. In 2009, John Shaw made a similar comparison between the maritime and space domains when arguing for a new space strategy based on the US Maritime Strategy. John Shaw, "Guarding the High Ocean: Towards a New National-Security Space Strategy through an Analysis of US Maritime Strategy," *Air & Space Power Journal* (*ASPJ*) 23, no. 1 (Spring 2009): 55–65, https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-23_Issue-1-4/2009_Vol23_No1.pdf.

39. Charles Hill, "Digital Piracy: Causes, Consequences, and Strategic Responses," *Asia Pacific Journal of Management* 24, no. 1 (March 2007): 9–25, https://econpapers.repec.org/article/kapasiapa/v_3a24_3ay_3a2007_3ai_3a1_3ap_3a9-25.htm.

40. There is some debate over the extent to which transnational criminal organizations would aid terrorist groups and vice versa. While financial gain might be a compelling reason for criminal groups to get involved in certain political activities, they also must confront the possibility of receiving greater attention from the state. The debate will likely resurface over potential threats to space. For different perspectives on this debate, *see* Christopher Dishman, "Terrorism, Crime and Transformation," *Studies in Conflict & Terrorism* 24, no. 1 (2001): 43–58, https://cco.ndu.edu/BCWWO/Article/980805/6-terrorist-and-criminal-dynamics-a-look-beyond-the-horizon/; Thomas Sanderson, "Transnational Terror and Organized Crime: Blurring the Lines," *SAIS Review of International Affairs* 24, no. 1 (Winter-Spring 2004): 49–61, https://www.researchgate.net/publication/236822940_Transnational_Terror_and_Organized_Crime_Blurring_the_Lines; Tamara Makarenko, "The Crime-Terror Continuum: Tracing the Interplay between Transnational Organised Crime and Terrorism," *Global Crime* 6, no. 1 (February 2004): 129–45, https://www.semanticscholar.org/paper/The-Crime-Terror-Continuum%3A-Tracing-the-Interplay-Makarenko/b350d8bdef812685cf71fdd663061d0478a7fce7; and Rajan Basra and Peter Neumann, "Criminal Pasts, Terrorist Future: European Jihadists and the New Crime-Terror Nexus," *Perspectives on Terrorism* 10, no. 6 (December 2016): 25–40, http://www.terrorismanalysts.com/pt/index.php/pot/article/view/554/.

41. According to the North Atlantic Treaty Organization (NATO) website, there were no successful piracy attacks between 2012 and when Operation Ocean Shield ended on 15 December 2016. NATO, "Counter-Piracy Operations," 19 December 2016, https://www.nato.int/cps/en/natohq/topics_48815.htm. *See also* European Union Naval Force Operation Atalanta, https://eunavfor.eu/mission/.

42. Michael Viets, "Piracy in an Ocean of Stars: Proposing a Term to Identify the Practice of Unauthorized Control of Nations' Space Objects," *Stanford Journal of International Law* 54, no. 2 (Summer 2018): 159–212, https://web.a.ebscohost.com/abstract?direct=true&profile=ehost&scope=site&authtype=crawler&jrnl=07315082&AN=130412326&h=RQIqNExyPac%2f%2bMgBed%2fTKcUBdfYKt54N1VipcdU4eX0EBadckn6hAlEz87NxQ5OF7li0Szl7cdxXQAN2m36L5A%3d%3d&crl=c&resultNs=AdminWebAuth&resultLocal=ErrCrlNotAuth&crlhashurl=login.aspx%3fdirect%3dtrue%26profile%3dehost%26scope%3dsite%26authtype%3dcrawler%26jrnl%3d07315082%26AN%3d130412326.

43. The US responded largely on its own to the 2014 hacking of Sony Pictures. The US filed formal charges against the individual believed to be responsible (acting as an agent of the North Korean government) and updated its laws to help law enforcement respond to cybercrimes. Brian Barrett, "DOJ Charges North Korean Hacker for Sony, Wannacry, and More," *Wired*, 6 September 2018, https://www.wired.com/story/doj-north-korea-hacker-sony-wannacry-complaint/.

44. Kristina Wong, "Rumsfeld Still Opposes Law of Sea Treaty," *Washington Times*, 14 June 2012, https://www.washingtontimes.com/news/2012/jun/14/rumsfeld-hits-law-of-sea-treaty/.

45. David Livingstone and Patricia Lewis, "Space, the Final Frontier for Cybersecurity?," research paper (London: Chatham House International Security Department, September 2016), https://www.chathamhouse.org/sites/default/files/publications/research/2016-09-22-space-final-frontier-cybersecurity-livingstone-lewis.pdf/.

46. John Hyten made a similar call in 2002 about the need to better prepare for all future conflicts in space, whether involving states, companies, or individuals. He argued that while the US should not yet deploy weapons to space, it needs to expedite its efforts to develop them. John Hyten, "A Sea of Peace or a Theater of War: Dealing with the Inevitable Conflict in Space," *ASPJ*

16, no. 3 (Fall 2002): 78–92, https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-16_Issue-1-4/Fall02.pdf.

47. Jervis, "Cooperation under the Security Dilemma"; Sean Lynn-Jones, "Offense-Defense Theory and its Critics," *Security Studies* 4, no. 4 (Summer 1995): 660–91, https://www.tandfonline.com/doi/abs/10.1080/09636419509347600; Stephen Van Evera, "Offense, Defense, and the Causes of War," *International Security* 22, no. 4 (Spring 1998): 5–43, https://www.jstor.org/stable/2539239?seq=1#page_scan_tab_contents; and Charles Glaser and Chaim Kaufmann, "What is the Offense-Defense Balance and How Can We Measure It?," *International Security* 22, no. 4 (Spring 1998): 44–82, https://www.belfercenter.org/publication/what-offense-defense-balance-and-how-can-we-measure-it.

48. The US legal system, for instance, does not distinguish between someone who attacks a civilian and someone who attacks a military target when such activities occur within the United States. For example, the legal system did not view the 2007 plot to attack Fort Dix, New Jersey as inherently different from the 2016 plot to attack a Garden City, Kansas apartment building and a mosque. In both cases, the plotters faced life in prison for the planned attacks. "Brothers Sentenced to Life in Prison for Alleged Plot against US Army Base," *Guardian*, 29 April 2009, https://www.theguardian.com/world/2009/apr/29/fort-dix-terrorism-attack-brothers-sentenced; and Tom Dart, "Kansas Men Face Life in Prison for Alleged Terrorist Plot against Somali Immigrants," *Guardian*, 17 October 2016, https://www.theguardian.com/us-news/2016/oct/17/kansas-terrorism-plot-somali-immigrants-trial.

49. The FBI definition of terrorism is: "the unlawful use of force or violence against persons or property to intimidate or coerce a Government, the civilian population, or any segment thereof, in furtherance of political or social objectives." US Department of Justice, Federal Bureau of Justice, *Terrorism in the United States 1998* (Washington, DC: Government Publishing Office, 1998), 28 C.F.R. Section 0.85. Interestingly, the NATO definition of terrorism is more similar to this than it is to the DOD definition in terms of including attacks against property.

50. The DOD definition of *terrorism* is: "the unlawful use of violence or threatened violence, often motivated by religious, political, or other ideological beliefs, to instill fear and coerce governments or societies in pursuit of goals that are usually political." Joint Staff, *Joint Publication 1-02*, Department of Defense Dictionary of Military and Associated Terms, 15 February 2016, s.v. "terrorism," https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf/.

51. Miller, "Terrorist Decision Making and the Deterrence Problem," 132–51.

52. Harrison et al., "Space Threat Assessment."

Gregory D. Miller, PhD

Dr. Miller (PhD, The Ohio State University) is an associate professor of Leadership Studies at the Air Command and Staff College at Maxwell AFB, Alabama.