The Remote Sensing Revolution Threat

LTC Brad Townsend, USA

Abstract

Remote sensing—using satellites to image objects on the ground—is rapidly evolving from primarily a strategic intelligence threat to national security to an operational threat to military forces. Remote sensing will further complicate the already well-understood intelligence and targeting threat created by drones and other battlefield sensors. Imminent remote sensing technologies will allow near real-time observation of military forces anywhere, at any time, and under any conditions. Ubiquitous observation will provide an overwhelming military advantage to the nation best able to leverage it while denying that capability to others. The current diplomatic, regulatory, and military means for managing this threat are inadequate for the level of challenge that these sensors will present to modern warfare. This article assesses the weaknesses in existing US approaches to managing the remote sensing threat. It then proposes a combination of novel diplomatic approaches and increased regulatory control measures that will complement future active military means of addressing the emerging threat of ubiquitous remote sensing.

*****

Early on the morning of 8 January 2020, as many as 10 Iranian missiles struck al-Assad Air Base in Iraq, a major hub of US military activity in the region.[1] That same day, news outlets worldwide commented on the apparent effectiveness of the Iranian missiles and the implications of the damage caused by the strikes. Much of this commentary and analysis used high-quality satellite imagery—provided by the US-based and licensed company Planet—taken in the hours after the attack. The photos allowed the world to see the extent of the damage and judge the relative accuracy of the strikes.[2] This episode was a watershed moment in the history of space. A US-based commercial remote sensing company had just released detailed, same-day satellite images of the effects of war between the US and a foreign power.

Iran also gained vital information that it might otherwise not have had on the effectiveness of its strikes and targeting. Using this imagery, Iran

could conduct poststrike analysis to refine its targeting for future strikes, presenting an even greater risk to US and Iraqi forces. Without Planet's satellite data, Iran would have had access only to fragmented and unconfirmed reports from eye-witnesses on the ground. Alternative means of gathering overhead imagery, such as the use of aircraft or drones, likely would have failed as neither Iraq nor the US would have allowed Iran to overfly al-Assad Air Base uncontested. Ultimately, Iran chose not to conduct follow-up strikes and further escalate the conflict, mitigating any potential damage that Planet's imagery could have caused. However, the swift public release of high-quality satellite imagery of an attack on US forces signaled the beginning of a new era in warfare—one that brings significant challenges, risks, and opportunities to future war fighting.

The opportunities inherent in having access to real-time imagery are easy to grasp. However, addressing the threat of high-quality, high-revisit rate, space-based remote sensing data in modern warfare is more complicated. It will require a tailored approach with military, regulatory, and diplomatic aspects. This article addresses existing and possible regulatory and diplomatic approaches while leaving the details of purely technical military options for dealing with the threat for future analysis. First, it discusses the development of remote sensing, trends in the rapidly evolving remote sensing market, and the effects of these trends on future war fighting. It then highlights current regulatory controls that can help mitigate the risk from domestic and allied commercial satellite imagery while balancing industry needs and national security. Finally, the article outlines the challenges of controlling third-party remote sensing through diplomatic means and proposes an approach to managing the third-party threat when diplomacy is inadequate.

Remote Sensing Development, Trends, and the Future of War Fighting

Remote Sensing Development

Before the advent of satellites, obtaining detailed intelligence on enemy locations and disposition during a conflict required risky overflights or the use of ground-based reconnaissance. Outside of conflict, getting overhead imagery of other nations for intelligence purposes was even more difficult without satellites, as nations jealously guard their sovereign airspace. For decades the satellites that acquired this valuable overhead intelligence were expensive, few, and controlled by only a handful of nations. In the last decade, advances in commercial technology have led to a proliferation of

remote sensing technology, with at least 25 nations now possessing some remote sensing satellites of various quality.[3] For countries without national platforms, high-quality imagery is readily available from commercial sources. The democratization of remote sensing information represents a new and real threat to military forces that only adds to the future battlefield's increasing complexity. There are some overarching trends in remote sensing satellite development, and they represent a substantial threat to future military operations.

With the advent of remote sensing in the 1960s, satellites could largely replace aircraft overflights for intelligence gathering purposes, but not without limitations. While a satellite can pass freely overhead in its orbit, it cannot reasonably change its orbit to pass over a specific target sooner. Thus, space-based intelligence is dictated by time limitations (temporal resolution) that are exacerbated by cost and target resolution limitations (spatial resolution).[4] Once digital return was possible and imagery satellites were no longer single use, a balance needed to be struck between resolution and on-orbit lifetime. Imagery satellites are, or at least were, ruinously expensive, so they needed to be high enough in their orbits to avoid a level of atmospheric drag that would limit their on-orbit lifetime. Higher altitudes drove the need for larger and more exquisite optics to ensure that spatial resolution remained relevant, further increasing costs. These high costs made space-based intelligence a privilege limited to the handful of nations that could afford to build, launch, and operate remote-sensing satellites. Because space-based imagery remained expensive, the number of commercial platforms remained relatively small, limiting their operational impact.

This began to change in 2001 when relatively high-resolution imagery became readily available for purchase by third parties with the launch of QuickBird-2 and the advent of highly capable and fully commercial remote sensing satellites. The first to break the .5-meter resolution barrier was the US-based DigitalGlobe's WorldView-1, launched in 2007. WorldView-1's capabilities were exceeded by WorldView-3's in 2014. This satellite could capture images at a .3-meter panchromatic resolution, but it cost nearly $600 million and had a best-case revisit rate to anywhere in the world of just over one day.[5] The most recent commercial satellite to follow this exquisite model was WorldView-4, which launched in 2016 and failed on orbit in early 2019—only two years into an expected 10-year lifespan.[6] These satellites returned high-resolution imagery but were limited by various technical factors to imaging 680,000 km^2 per day, an area roughly equivalent to the size of Texas.[7] With high spatial resolution but low tem-

poral resolution, these satellites were valuable intelligence tools but remained a relatively small operational risk to military forces in the field.

Increasing temporal resolution requires launching more satellites, but the technical limitations discussed above made doing so cost prohibitive as long as launch costs remained high. Only since 2015 have launch costs begun to fall in real terms as true commercial companies, most notably SpaceX, entered a market previously dominated by near national monopolies. These national monopolies relied primarily on domestic government contracts for funding and had no real competition, so they had little incentive to attempt revolutionary innovation. Beginning with NASA's Commercial Orbital Transportation Services (COTS) contract that essentially provided seed funding for SpaceX, real commercial competition entered the launch market for the first time, leading to dramatic technological leaps that have opened new market opportunities.

Remote Sensing Trends

A paradigm shift occurred with the drop in launch costs that coincided with a rapid shift toward satellite miniaturization. Miniaturization altered the economics of satellite construction, leading to a revolution in satellite imagery. Smaller satellites are cheaper. Dozens can be launched simultaneously into a single orbital plane, where careful manipulation of the space environment places them in useful configurations and decreases temporal resolution. The tradeoff is that remote sensing satellites launched in this way are individually much less capable of hosting large optical payloads, reducing their spatial resolution. Small remote sensing satellites compensate by being launched into much lower orbital altitudes—250 km versus 600 km or more for DigitalGlobe's more traditional WorldView satellites. However, the increased atmospheric drag on satellites in these orbits substantially reduces their lifetime. Thus, maintaining a constellation requires these small satellites to be frequently replenished. The shortened replacement cycle drives a demand for more satellites and launches, reduces unit cost, and allows for iterative improvements of both. These benefits further reinforce the economic incentives associated with this approach. A race is on to achieve the best spatial and temporal resolution possible. In late 2017, the US-based company Planet attained the goal of imaging the entire earth's surface at a 3–5 meter resolution in a single day.[8] Most would have considered this paradigm-shifting achievement impossible just a few years earlier. It was one of these relatively cheap satellites that provided the initial imagery of al-Assad Air Base. Planet is not alone in introducing disruptive approaches to remote sensing. Dozens of new imagery provid-

ers have begun to enter the market, offering a variety of capabilities from synthetic aperture radar (SAR) to hyperspectral imaging capabilities. As of 2021, many of these systems are already on orbit in small numbers as the first tranche of future constellations of similar satellites. The end state of this race between commercial companies and nations leveraging commercial technology is ubiquitous high-resolution coverage of the entire globe at all times. This resolution convergence will undoubtedly occur before 2030. However, hints of the war-winning nature of ubiquitous observation in modern warfare have already been demonstrated in the recent conflict between Armenia and Azerbaijan, albeit by airborne rather than space-based sensors.

Effects of Remote Sensing Trends on Future War Fighting

In late 2020, Armenia and Azerbaijan fought a small but intense conflict over the contested region of Nagorno-Karabakh demonstrating that that long-range precision strikes and indirect fire aided by overhead intelligence can be a war-winning combination. At the outset of the conflict, Armenia was considered a conventionally superior military to Azerbaijan with better training and leadership.[9] Even so, it was quickly outclassed by Azerbaijan's tactical use of drones to provide targeting data to Azerbaijan's artillery and other long-range precision weapons. Initially, Armenia operated a Russian-built air defense system that Azerbaijan needed to eliminate to fully use its Turkish- and Israeli-provided drone capability.[10] Azerbaijan was forced to use 11 unmanned Soviet-era AN-2 aircraft as bait to get the Armenian air defenses to fire so that it could identify and eliminate them.[11] Once Azerbaijan neutralized the air defenses, it could use drones to track and then destroy Armenian forces on the ground. By some counts, Azerbaijan destroyed nearly 1,000 tanks, armored fighting vehicles, and other vehicles during the short campaign using this precision fire, forcing Armenia to sue for peace.[12] Azerbaijan's success in using drones to provide targeting data to its indirect fire weapons offered a glimpse of future warfare.

Despite its success in the Nagorno-Karabakh conflict, drone warfare is not without limitations that satellite-based intelligence could overcome or augment. First, Azerbaijan defeated Armenia with airborne platforms that had limited fields of view and were subject to weather limitations on operations—constraints that would not impact satellites. Second, Russia quickly fielded a new counter-drone electronic warfare system, Krashukha-4, which successfully downed Turkish drones over ranges of up to 300 km.[13] This quick and effective counter to unmanned airborne platforms demonstrated their vulnerability to electronic warfare. Clearly,

electronic warfare will be applied to satellites should they become a threat as well, but unlike air-breathing drones, they are not immediately vulnerable to physics. The targeting picture against satellites will also be far more complex with various foreign and commercial platforms passing overhead simultaneously, which may or may not be aiding an adversary. Finally, within the conflict zone, the warring parties were able to declare a no-fly zone. This ability—not possible in orbit—greatly aided their capacity to identify and track potential hostile targets.[14]

The exact particulars of any one conflict are never repeated, as circumstances, terrain, and technology are constantly evolving. However, one can draw several predictions from Nagorno-Karabakh on how more capable opponents will fight in the future. First, the larger lesson from this conflict is that the vast majority of combat losses in nation-state conflict continue to come from indirect fire and other long-range weapon systems.[15] Second, the ability to accurately track and target your opponent is critical to the effectiveness of these systems, so the side that has the better intelligence will be able to eliminate its opponent faster. Finally, preventing your opponent from saturating the battlespace with sensors—whether drones or other unmanned systems—will be a critical priority for the defender. In sum, the side that can best fuse intelligence with long-range precision fires will dominate the battlefield.

The role of real-time intelligence from remote sensing satellites in a future conflict will be akin to that of drones in gathering targeting intelligence for Azerbaijan. The proliferation of commercial and national remote sensing capabilities to image broad areas in detail and relay that information back to fire direction centers will be a new critical node in the kill chain. Commercial providers are already working on real-time tasking and response from satellites.[16] Purpose-built national efforts like the Space Development Agency's tracking and transport layer will surely be even more capable than commercial systems and critical to tactical success on the future battlefield.[17] The ever-decreasing spatial and temporal resolution of remote sensing satellites will bring space-based intelligence forward from its use as a historically strategic-level tool to a tactical tool. Mitigating this shift will require a mixture of active, passive, regulatory, and diplomatic tools.

Approaches and Options

The effect of a resolution convergence on military operations will become impossible to ignore over the next decade. As space-based remote sensing platforms transition from primarily an intelligence risk to a real-

time operational risk to military forces, effective methods of managing these systems will be necessary. Active military means of targeting remote sensing satellites will be a key future element of managing this threat. Already, Russia and China are developing ground-based laser systems designed to counter remote sensing systems in lower orbits.[18] These systems will likely be an effective counter to an opponent's remote sensing platforms. Nevertheless, the threat picture in orbit is much more politically complex than in an airborne environment. The nature of orbital mechanics means that remote sensing platforms from dozens of nations and commercial entities will transit any conflict zone daily. For relatively diplomatically isolated nations, such as Russia or China, engaging every satellite not belonging to a direct ally using active military means will be a real possibility. However, a less diplomatically isolated nation like the US—which historically prides itself on its alliances and generally adheres to international law—will find it much more difficult to engage in indiscriminate use of active military means. As a result, a much more nuanced approach to managing the satellite threat that mixes novel diplomatic and regulatory measures with active military means is needed. Discussed next are existing and potential new approaches to managing the threat outside of active military means.

Active measures are needed against adversary remote sensing systems, but they should be a last resort against domestic commercial systems or those owned by third parties. These systems still represent an operational threat since the imagery they capture can become publicly available or accessible for purchase and give an adversary valuable intelligence. In situations where the adversary nation has no significant domestic remote sensing capability, the active measures discussed above are largely unnecessary. Instead, a combination of regulatory and diplomatic options becomes the primary method of limiting the distribution of valuable overhead intelligence.[19] Currently, the US has the largest commercial remote sensing market and is likely to continue to lead the market due to an increasingly friendly regulatory structure, a robust industrial base, and lucrative government contracts. The remaining global commercial market will likely remain concentrated in close US allied and partner countries. Thus, the US is presented with particular difficulties in managing these remote sensing threats because using active military measures against domestic or allied commercial systems is not a politically palatable option. However, it is possible to use the US regulatory structure and other methods to control domestic commercial remote sensing. Also, diplomatic measures accompanied by reciprocal agreements and international notifications could be

an effective control measure for allied and third-party systems. A combination of these regulatory and diplomatic controls could be effective complements to military means of controlling remote sensing intelligence, limiting the inadvertent operational and intelligence risk that these systems represent.

US Commercial Remote Sensing Systems

Regulatory controls. US regulation of commercial remote sensing systems began in 1984 with the passage of the Land Remote Sensing Commercialization Act.[20] This act was primarily intended to privatize the Landsat program, but it also included provisions to allow the secretary of commerce to issue licenses for commercial remote sensing satellites. The Department of Commerce quickly delegated this authority to the National Oceanic and Atmospheric Administration (NOAA), where it has remained.[21] While the 1984 act was far from perfect, it established a framework for licensing commercial remote sensing systems and included many of the philosophical underpinnings of the current law. The 1984 act was superseded in 1992 by the Land Remote Sensing Policy Act, which removed some of the more egregious licensing conditions, including the ability of the secretary of commerce to "terminate, modify, condition, transfer, or suspend licenses" without any legal recourse for the licensee.[22] Included without substantive change in an updated 2010 National and Commercial Space Programs legislation, the 1992 act remains the foundational legal basis of US remote sensing licensing.

The basic tenants of the 1992 remote sensing act are relatively benign but do include several national security caveats. As part of the law, a US licensed commercial operator must employ "the system in such a manner as to preserve the national security of the United States and to observe the international obligations of the United States."[23] Further, a licensee is required to inform the secretary whenever entering into any agreement "with a foreign nation, entity, or consortium involving foreign nations or entities."[24] Other basic requirements include providing the orbital characteristics of the system, satisfactorily disposing of the satellite, and informing the secretary of any deviations to its orbit. At the surface level, it seems reasonable to request that a commercial provider comply with these requirements due to the US's international obligations concerning debris tracking and national security. Where ambiguity quickly presents itself is with what is meant by the requirement to operate in a manner that preserves national security. Commercial providers and various government

agencies are very likely to have different interpretations of what constitutes protecting national security.

The Planet imagery example mentioned earlier illustrates this conflict of interest and opinion. Using these images, Iran could judge the effectiveness of its targeting systems and the impact of its strikes on specific targets on al-Assad—a clear national security risk. Alternatively, the rapid release of detailed imagery into the public sphere allowed the American people and the international community to independently determine that the number of missile strikes and the amount of damage was limited. This information served to calm media speculation and support the narrative that the missile strike was merely a face-saving exercise for Iran—a clear national security gain.[25] Planet's release of imagery could then have different national security interpretations depending on perspective and subsequent actions. In this case, Iran did not conduct follow-up strikes. Thus, in hindsight, Planet's release of imagery did not harm national security. This case demonstrates the ambiguity behind the seemingly straightforward requirement to preserve the national security of the US levied on commercial imagery providers.

If the US government had chosen to exercise regulatory control over Planet and restrict the release of its imagery, the regulatory options are limited. Presidential Decision Directive 23 (PDD-23), signed by President Bill Clinton in 1994, introduced the concept of modified operations colloquially known as "shutter control." PDD-23 stipulated that commercial imagery providers might be required "during periods when national security . . . may be compromised, as defined by the Secretary of Defense or the Secretary of State, respectively, to limit data collection and/or distribution by the system to the extent necessitated by the given situation."[26] Shutter control is a powerful regulatory tool that the US government could enact to prevent US licensed commercial providers from imaging everything from an individual air base to an entire theater of military operations. However, despite its usefulness as a regulatory tool, shutter control has never been invoked.

Challenges of implementing regulatory controls. The challenges of enforcing shutter control have likely prevented its implementation. First, doing so would almost certainly trigger a legal challenge. A legal challenge would probably not come from the licensed satellite owner. Instead, it would likely emerge from news agencies or other entities seeking access to the denied imagery—unless there was broad consensus that the justification for invoking shutter control demonstrably supported national security. As in the Planet example, proving the requirement for shutter control

is difficult under even the most seemingly clear-cut circumstances. Second, the use of shutter control could have long-term repercussions on the health of the US commercial remote sensing industry. It would demonstrate the vulnerability of US-licensed providers to government interference, potentially making the US a less attractive licensing environment.

Logistical challenges also present obstacles to invoking and verifying the effective execution of shutter control. With the growing number of remote sensing license holders in the US, active verification of compliance is not reasonably possible. The government would effectively be reliant on voluntary compliance from license holders. Given that the civil penalty cap the secretary of commerce can impose on an imagery provider for violating the terms of its license is only $10,000, a licensee might simply decide that the cost of compliance is more than the price of the punishment.[27] A provider could also maliciously conclude that the value of the shutter-controlled imagery is worth much more than the fine and sell it despite the government order. This scenario is possible, though doubtful, despite the relatively low civil penalty. The US government is the largest single purchaser of commercial satellite imagery with the EnhancedView contract with the US National Reconnaissance Office (NRO) alone worth $300 million per year for Maxar technologies.[28] In an industry with an estimated global revenue of just $2.2 billion, US-based imagery providers are unlikely to risk the possibility of lucrative future contracts with the US government by intentionally ignoring shutter control requests.[29]

A final obstacle to invoking shutter control is a recently released regulatory structure that does not explicitly require that all US-licensed remote sensing providers be subject to shutter control. This new regulation, the first revision since 2006, relies on a tiering structure determined primarily by foreign availability benchmarks.[30] Under this regulation, if a remote sensing capability is marketed for purchase from any foreign supplier, it is considered available. The US provider is then placed in the lowest of three possible regulatory categories, tier one. Within tier one, remote sensing providers are still required to operate their systems "to preserve the national security of the United States," but they are not subject to shutter control.[31] If a remote sensing capability is common only to other US-licensed providers or is unique, it is placed in tier two or tier three, respectively. As foreign availability grows, a larger percentage of highly capable remote sensing systems will no longer be subject to shutter control directives. The secretary of defense can still overrule the availability determination based on national security concerns, but exercising this authority will likely be difficult and rare given the political implications.[32] Despite these

regulatory restrictions on shutter control, it remains in law as a capability that the US can invoke, though the new regulatory structure will make its broad implementation extremely difficult. Even so, shutter control is a powerful regulatory tool for controlling domestically licensed remote sensing systems, but an alternative approach is necessary for foreign commercial systems.

Foreign Commercial Remote Sensing Systems

Foreign commercial remote sensing systems are categorized as allied, third party, or partly adversary owned—with each requiring a slightly different approach.

Allied commercial systems. Allied systems can be addressed through diplomatic channels. However, the degree of control that allied countries have over their remote sensing industry varies, and any request would have to be matched by restrictions on US commercial companies. Canada is an example of a nation with remote sensing regulations that closely mirror those of the US, including a provision that the minister of defense can "interrupt or restrict" the operations of a licensee on national security grounds.[33] This language is essentially mirrored in US law, which grants the secretary of defense the ability to direct modified operations (shutter control) of US licensees. With its regulatory structure, Canada, as a close ally of the US, would be receptive to and capable of limiting the operations of its satellites upon request using its similar regulatory mechanisms. However, it would certainly expect reciprocal restrictions on US systems. While Canada uses the same basic approach to security as the US, with modified operations directives used at the discretion of the Defense Department, not all Western nations take the same regulatory approach.

Germany takes a different approach to remote sensing regulation than either the US or Canada. German law for remote sensing platforms is sensitive to the possible use of German commercial imagery for military purposes and its impact on domestic security and foreign policy. The country's regulations require licensed operators to conduct a sensitivity check of all data transactions against a government database, taking into account data quality, target area, and the individual making the request.[34] Transaction controls avoid the complexities of attempting to regulate the technical aspects of remote sensing systems as the US has done and instead focuses on controlling the product. This control by the German government would allow for a quick response if it judged a request by a foreign government to limit the release of imagery to be valid. Since German remote sensing law is intended to support the national commitment to peace and is sensitive to

endangering foreign security interests, Germany would likely be among the most receptive nations to diplomatic requests to limit imagery distribution. Alongside France, Germany is one of just two European Union (EU) members with an overarching national policy governing remote sensing.

Managing the remote sensing security threat through diplomatic means with the broader European Union presents a more challenging problem than with Germany or France. Outside of the US, the member states of the European Union collectively have the largest commercial and privatized remote sensing market, with some smaller members such as Finland possessing highly capable commercial providers. Remote sensing companies based in these less-regulated EU member states present a much more difficult challenge since the EU does not have clear overarching policies governing remote sensing. The lack of an EU-wide regulatory mechanism for controlling the release of satellite imagery to protect domestic or foreign national security is problematic. Even if the nation receiving the diplomatic overture accepts a request as valid, it may find it legally impossible to impose any sort of limiting controls on the providers based within their borders. If allied nations lack an adequate regulatory framework or the legal authority to prevent their commercial providers from releasing imagery, then individual providers must be treated in the same manner as third-party commercial systems.

Third-party commercial systems. The second category of foreign commercial remote sensing systems is third-party commercial systems. They present a challenge for any nation attempting to deny observation of military operations. Unlike products from third-party national systems—which are unlikely to be shared outside the owning government due to concerns over revealing capabilities and limitations—commercial providers operating from neutral nations will likely consider hostilities between other nations as an opportunity. Operationally this means that they are just as much a threat as adversary systems, but active measures cannot be used against them without a careful assessment of the risk of angering the host nation. Diplomatic overtures would seem to be the best approach and certainly a necessary step in limiting the release of data from third parties, but alone they are unlikely to be effective or timely. Neutral nations may be slow in responding to diplomatic overtures for innocent or malicious reasons. Once hostilities have begun, the normally slow pace of the diplomatic process will likely create unacceptable risk. Historically, the US has successfully applied this diplomatic approach just once before, and it is unlikely to work again. This was during the Gulf War when the United Nations, at US urging, mandated an embargo on satellite imagery sales to

Iraq.[35] The only available non-US imagery was from France's SPOT satellite, and the agreement required SPOT to forgo sales to media companies to avoid the inadvertent release of imagery to Iraq through third parties. SPOT had a relatively low 10-meter resolution at the time but could still have provided valuable overhead intelligence to the Iraqi government, which also had lost access to aerial reconnaissance.[36] This embargo on the sale of imagery to Iraq worked and allowed the US to successfully execute the "left hook" maneuver that outflanked and surprised the Iraqi Army.

Replicating the same diplomatic embargo would be orders of magnitude more difficult today than it was in 1990. At that time, only a single close ally had a commercial capability that presented a threat. The threat today is proliferated across many nations, with imagery commercially available from most major US allies, third parties, and potential US adversary China.[37] It is doubtful that in the future the US could successfully request a United Nations embargo or that it could be enforced with the same degree of success achieved during the Gulf War. An alternative to negotiations is to develop a mechanism that provides notice yet is quick and effective at warning operators that imaging of specified areas is not authorized and would risk damaging or interfering with the imaging satellite. Aviation notices to Airmen (NOTAM) offer a possible framework for how this mechanism could effectively function.

NOTAMs provide aircraft with information in an internationally recognized format warning of hazards or airspace restrictions. They are an outgrowth of the Convention on International Civil Aviation hosted by the US in 1944 that established international guidelines for civil aviation. The convention does not apply to military aircraft, but the resulting regulatory mechanisms and processes are generally adhered to by military aviation during normal operations. Among the guidelines in the convention is an understanding that civil aircraft operating for non-civil purposes in the airspace of a nation may be dealt with by "any appropriate means."[38] It is a stretch to translate this understanding and its meaning into the space domain. Still, a similar agreement applied to space systems could provide the legal framework for nations to interfere with the operations of third-party commercial satellites, which become threats to security when transiting over sovereign territory. For military operations outside of sovereign territory, which is more likely for the US, the NOTAMs mechanism could simply provide clear and unambiguous warning that third-party systems should not image an area. Systems that violate this notice by pointing their optics at Earth in these areas may be damaged by active

directed-energy weapon systems or, in the case of SAR systems, may be actively interfered with if they are detected radiating energy.

Adversaries with an ownership stake. Commercial systems that an adversary has a significant ownership stake comprise the third category of commercial systems that might necessitate a diplomatic or regulatory approach. This category is not as clear-cut as it first seems. The international consortiums that operate many commercial systems may be partially owned by companies based in the territory of both sides in a conflict. Multiparty ownership creates an added difficulty for determining the degree of aggressiveness in managing these satellites. Some commercial providers will be based in an adversary's territory and have contracts with their host government, making them equivalent to adversary national assets. For other commercial systems, the threshold for treatment as an adversary system is difficult to discern. Determining a threshold for designation as an adversary-controlled system will ultimately require a judgment call at the national level, which balances the diplomatic risk against the operational risk of taking active measures. Figure 1 summarizes approaches to allied, third-party, adversary, and US commercial satellite remote sensing systems.

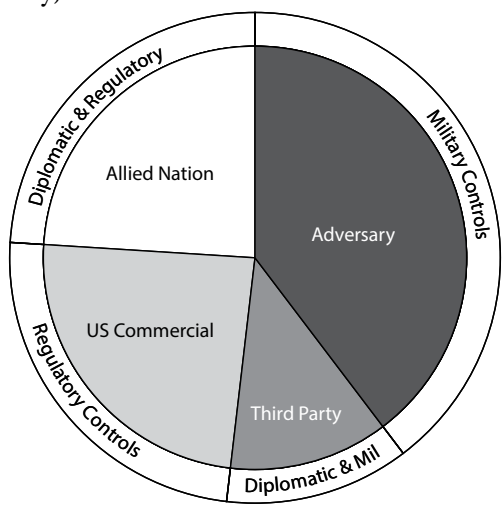

Figure 1. Approaches to remote sensing. Each remote sensing satellite will need to be managed broadly by category.

A New Approach to Mitigating Third-Party Threats

Diplomatic and regulatory approaches to controlling the release of remote sensing data are a necessary complement to active and passive military measures (table 1). However, no simple solution exists to mitigate the operational risk from non-adversary remote sensing satellites. Diplomatic

means are the best approach with allied commercial systems, while third-party systems may require a more aggressive approach. Further, complexities in determining the risk posed by commercial systems, as well as by assigning ownership, present a formidable challenge. Cutting through the complexity by developing and exercising a NOTAM-type mechanism—in this case, a notice to Spacemen (NOTSM)—to protect sensitive military operations is the most straightforward approach, but it requires enforcement. This enforcement requires dedicated on-site assets capable of tracking and engaging any ISR asset transiting overhead with destructive and nondestructive effects. A comprehensive and intensive multipart strategy that includes both diplomatic and active measures is a challenging but necessary part of limiting the impact that non-adversary remote sensing can have on military operations.

		Level of War		
		Peacetime	*Tension*	*Conflict*
Satellite Owner	*Adversary national and commercial*	Passive measures (denial and targeted deception)	Increased passive measures (denial and targeted deception) Dazzling plus limited nondestructive interference	Nondestructive: cyberattacks, jamming of links Destructive: lasers, ASATs and other space weapons
	Third party	Passive measures (denial)	NOTAMs and diplomatic efforts	NOTAMs escalating to dazzling and nondestructive attacks
	Allied national and commercial	Passive measures (denial) Shared regulatory controls	Diplomatic efforts	Continued diplomatic efforts, NOTAMs escalating to nondestructive in the event of serious security violation
	US Commercial	Regulatory limitations on highly capable systems plus passive measures	Shutter control	Shutter control

Table 1. Methods of control. Example measures that can be applied across the spectrum of conflict to control remote sensing. Note that measures build from right to left, though that does not mean that peacetime control measures should cease in conflict.

Conclusion

The near-ubiquitous space-based observation of Earth is coming and cannot be ignored by military planners. Already an intelligence threat, remote sensing satellites are rapidly developing into an operational threat

to military forces. Passive-only measures of managing the risk from remote sensing satellites will become increasingly ineffective unless accompanied by active measures to limit the observation of friendly forces, such as those capabilities that China and Russia are already developing. [39] Where and when to apply active measures is an increasingly complex problem requiring a careful balance of diplomatic and operational risks since not all remote sensing threats are necessarily adversary controlled. Thus, some require diplomatic or regulatory methods of control.

Only a handful of nations possess a clear regulatory framework for managing domestic remote sensing threats. The US regulatory structure for commercial systems is robust. Still, it has shifted away from relying primarily on system-level technical limitations toward reliance on shutter control and broad language governing national security as its regulatory control mechanism. As a regulatory mechanism, shutter control is, in theory, an efficient tool for protecting national security. However, it is one that the US has never exercised for fear of legal challenges or doing harm to its domestic remote sensing industry. For allied nations, a patchwork of regulatory controls exists, which those nations may be willing to enforce when asked through diplomatic channels.

Managing the threat is most difficult for third-party systems or for those unwilling to accommodate foreign security concerns. In these cases, a NOTAM/NOTSM concept may be necessary to prevent observation. The NOTSM concept allows for appropriate forewarning that imagery of a specified area is not welcome and attempts to image the area will be met with an active response. Such a concept currently has no legal framework to rely on and would need to be declared unilaterally or developed as a norm acceptable over sovereign territory or regions with active combat operations. Either way, active measures against non-adversary satellites would require careful analysis of the associated risk.

Remote sensing satellites in an era of ubiquitous imagery will provide an overwhelming military advantage to the side that is best able to leverage them for its own gain while denying its opponent access. Despite this seemingly obvious conclusion, there seems to be relatively little acknowledgment of the threat that these satellites will pose to operational forces in the future. Remote sensing satellites that historically promoted strategic stability by allowing clear observation inside an adversary's borders are quickly developing into a critical enabling tool for future warfare. Full recognition of the scale of the threat and the opportunity that these systems present may not come until a nation can successfully exploit its advantage in using and controlling space to rapidly defeat a near-peer mili-

tary power. When that day arrives, military space will truly have come of age as a war-fighting domain. SSQ

LTC Brad Townsend, USA

Colonel Townsend serves as a space policy advisor on the Joint Staff. He is the author of *Security and Stability in the New Space Age: The Orbital Security Dilemma* (Routledge Press, 2020). He holds a PhD and MPhil in military strategy from the US Air Force's Air University School of Advanced Air and Space Studies. A 2002 graduate of the US Military Academy, he also earned an MS in astronautical engineering from the Air Force Institute of Technology and an MS in space operations management from Webster University.

Notes

1. Geoff Brumfiel, "Satellite Photos Reveal Extent of Damage from Iranian Strike on Air Base in Iraq," NPR, 8 January 2020, https://www.npr.org/.

2. Diana Stancy Correll and Aaron Mehta, "See the Damage at Al-Asad Airbase Following Iranian Missile Strike," *Military Times*, 8 January 2020, https://www.militarytimes.com/.

3. Jon B. Christopherson, Shankar N. Ramaseri Chandra, and Joel Q. Quanbeck, *2019 Joint Agency Commercial Imagery Evaluation—Land Remote Sensing Satellite Compendium* (Reston, VA: US Geological Survey, 2019), 41–43, https://pubs.usgs.gov/.

4. *Temporal resolution* refers to the amount of time required for a satellite or constellation to revisit a specific point on Earth's surface. For example, a satellite that passes over the same place once each day would have a temporal resolution of 24 hours. In contrast, two satellites in a constellation that each pass over the same spot once each day but 12 hours apart would have a temporal resolution of 12 hours. *Spatial resolution* refers to the quality of an image and for electro-optical imagery is synonymous with ground sample distance (GSD) or the midpoint of two adjacent pixels on a sensor when projected onto the ground. Spatial resolution is a broader term, as it also captures synthetic aperture radar technology and post-processing techniques to capture the best "picture quality" of a sensor.

5. Debra Werner, "WorldView-4's Long Road to Launch about to Pay Off for DigitalGlobe," *SpaceNews Magazine*, 15 August 2016, http://www.spacenewsmag.com/.

6. "DigitalGlobe Loses WorldView-4 Satellite to Gyro Failure," *SpaceNews*, 7 January 2019, https://spacenews.com/.

7. "WorldView-3 Satellite Sensor," Satellite Imaging Corp, accessed 19 January 2020, https://www.satimagingcorp.com/.

8. Robbie Schingler, "Planet Launches Satellite Constellation to Image the Whole Planet Daily," 14 February 2017, https://www.planet.com/.

9. Gustav Gressel, "Military Lessons from Nagorno-Karabakh: Reason for Europe to Worry," European Council on Foreign Relations, 24 November 2020, https://ecfr.eu/.

10. Michael Kofman, "Perspectives | Armenia's Military Position in Nagorno-Karabakh Grows Precarious," Eurasianet, 24 October 2020, https://eurasianet.org/.

11. Robyn Dixon, "Azerbaijan's Drones Owned the Battlefield in Nagorno-Karabakh — and Showed Future of Warfare," *Washington Post*, 11 November 2020, https://www.washingtonpost.com/.

12. Dixon.

13. "Russia Shot-Down A Total of Nine Turkish Bayraktar Drones Near Its Armenian Military Base — Russian Media Reports," *Eurasian Times*, 21 October 2020, https://eurasiantimes.com/.

14. "Armenia Declares No-Fly Zone in Armenia and Nagorno-Karabakh," Reuters, 12 November 2020, https://www.reuters.com/.

15. Gressel, "Military Lessons from Nagorno-Karabakh."

16. Debra Werner, "Capella Sends First Task Order through Inmarsat Data Relay," *Space News*, 23 November 2020, https://spacenews.com/.

17. Space Development Agency, "Transport," accessed 19 July 2021, https://www.sda.mil/.

18. Defense Intelligence Agency, *Challenges to Security in Space*, (Washington, DC: Defense Intelligence Agency, January 2019), 20, 29, https://www.dia.mil/.

19. There is risk that nations opposed to US actions will provide a disadvantaged opponent with imagery from national level systems. This risk is mitigated by the fact that nations are hesitant to provide third parties access to raw imagery and reveal national capabilities (and limitations) and by the time that making a decision to release even blurred imagery or intelligence to a third party requires. These practical limitations prevent this source of imagery from being a real-time operational threat but does present challenges from an intelligence perspective.

20. Land Remote-Sensing Commercialization Act of 1984, Pub. L. No. 98-365, 15 USC 4201 (1984).

21. Dorinda Dalmeyer and Kosta Tsipis, "USAS: Civilian Uses of Near-Earth Space," *Heaven and Earth* 16 (1997): 47.

22. Land Remote-Sensing Commercialization Act of 1984, sec. 403a(1).

23. Land Remote-Sensing Act of 1992, Pub. L. No. 102-588, 15 USC 5623 (1992), sec. 5622(b)1.

24. Land Remote-Sensing Act of 1992, sec. 5622(b)6.

25. Shane Harris et al., " 'Launch, Launch, Launch': Inside the Trump Administration as the Iranian Missiles Began to Fall," *Washington Post*, 8 January 2020, https://www.washingtonpost.com/

26. William J. Clinton, Presidential Decision Directive 23, "US Policy on Foreign Access to Remote Sensing Space Capabilities," 9 March 1994, Clinton Digital Library, https://clinton.presidentiallibraries.us/.

27. "Licensing of Private Land Remote-Sensing Space Systems," 15 CFR 960, Vol. 71, No. 79 § (2006), pt. 960.15.

28. Theresa Hitchens, "NGA Re-Ups Maxar Imagery Contract," *Breaking Defense*, 28 August 2019, https://breakingdefense.com/.

29. "Commercial Satellite Imaging Market Statistics, Trends | Forecast - 2026," Allied Market Research, accessed 5 May 2020, https://www.alliedmarketresearch.com/.

30. Licensing of Private Remote Sensing Space Systems, 15 CFR 960 (2020), Cornell Law School, https://www.law.cornell.edu/.

31. 15 CFR 960, sec. 960.8.

32. 15 CFR 960, sec. 960.6a.

33. Remote Sensing Space Systems Act (Canada), SC 2005, c. 45, sec. 14(5), https://laws-lois.justice.gc.ca/.

34. "National Data Security Policy for Space-Based Earth Remote Sensing Systems," Background Information for the Act on Satellite Data Security, Bonn, German Federal

Ministry of Economics and Technology, 15 April 2008, 5, https://www.bmwi.de/. Effective 1 December 2007.

35. Denette L. Sleeth, "Commercial Imagery Satellite Threat: How Can U.S. Forces Protect Themselves?" (master's thesis, Naval War College, 2004), 12.

36. "SPOT Medium Resolution Satellite Imagery," Apollo Mapping, accessed July 2021, https://apollomapping.com/.

37. Shankar N. Ramaseri Chandra, Jon B. Christopherson, and Kimberly A. Casey, *2020 Joint Agency Commercial Imagery Evaluation—Remote Sensing Satellite Compendium*, US Geological Survey (USGS) Circular 1468, ver. 1.1 (Reston, VA: USGS, October 2020), https://doi.org/10.3133/cir1468.

38. *Convention on International Civil Aviation,* doc. 7300/9, 9th ed. (Montreal: International Civil Aviation Organization, 2006), 3, https://www.icao.int/.

39. Defense Intelligence Agency, *Challenges to Security in Space*, 20.