

An Interoperable Information Umbrella: Sharing Space Information Technology

MARIEL BOROWITZ

Abstract

In 1996, Joseph Nye and William Owens foresaw the importance of information technologies and data sharing, warning that if the United States did not share the knowledge gained from its information systems—particularly satellites—other countries would have added incentive to develop their own. However, their analysis did not consider the potential benefits of resiliency offered by redundant allied systems. Decision makers should consider both the soft-power benefits of data sharing as well as the resiliency benefits associated with redundant, interoperable systems to enable a more robust path forward for gaining and preserving power in the information age. This article examines the disadvantages of restricting access to data as predicted by Nye and Owens and the unexpected benefits of redundancy for three space sector information technologies: reconnaissance satellites, global navigation satellite systems, and space domain awareness systems.

In 1996, Joseph Nye and William Owens argued that the United States was poised to lead the information revolution, increasing its power in international affairs. Key to maintaining its technological superiority, however, was sharing this information. They recommended that the US provide an “information umbrella,” sharing information to gain leverage with allies and maintain its leadership position. They noted that the United States has a considerable advantage in terms of investment and experience in these technologies and argued that if America did not share its knowledge it would create incentives for countries to develop independent capabilities. Conversely, its willingness to do so could be a way to build coalitions before aggression begins or to improve the decision-making of recipients during conflicts.¹

Nye and Owens suggested that the US “information umbrella” should follow the model of the “nuclear umbrella.” As with the nuclear umbrella, the information umbrella would provide leverage with allies and form the foundation for a mutually beneficial relationship. They acknowledged that this would require overcoming long-established prejudices against openly sharing intelligence. Concerns included the risks of disclosing sources and methods used in obtaining information and of making clear what the US did and did not know, potentially reducing its advantage. However, they concluded that “selectively sharing these abilities is therefore not only the route of coalition leadership, but the key to maintaining U.S. military superiority.”²

The comparison to the nuclear umbrella provides a useful example to envision the potential benefits of information sharing, particularly space information, but the comparison is not perfect. While development of nuclear weapons is tightly restricted by the Treaty on the Non-Proliferation of Nuclear Weapons, there is no such restriction for space information technology. Nor are the dangers associated with the proliferation of this technology considered nearly as dire. This factor complicates the ability to develop and maintain an information umbrella but also broadens the policy options available. In many cases, the United States may find it beneficial to share data and encourage the development of independent space systems among allies.

James Clay Moltz states that “net-centric” space technology, based on resiliency gained through redundant systems and commercial and international partnerships, may be more critical in today’s world than traditional views of power that emphasize purely national technologies. Further, Moltz contends that the United States is better situated than its potential adversaries to excel in this new form of power. The US has allies capable of developing and maintaining advanced space systems while its primary adversaries, Russia and China, have few, if any, close allies with this capability.³ This suggests that combining information sharing and coordinated space technology development to enable more capable and resilient interoperable systems may provide greater security advantages than information sharing alone.

This article examines the historical development of three military space sector information technologies—reconnaissance satellites, global navigation satellite systems, and space domain awareness systems—and demonstrates that in these areas Nye and Owens’s warning was prescient. The US reticence to engage in meaningful data sharing contributed to allies deciding to develop independent capabilities. However, the examined cases also

show that these developments resulted in unforeseen benefits to the United States in terms of redundancy and resilience that now play a critical role in US military power. These three cases indicate that the United States could have achieved benefits earlier, and with less tension among allies, if it had pursued a policy encouraging both information sharing and the development of interoperable systems. Lessons learned from these cases can be applied to future decision making.

Reconnaissance Satellites

The value of reconnaissance satellites has been evident since the beginning of the space age. The United States' first successful reconnaissance satellite mission, Corona, launched in 1960. This first satellite collected more imagery of the Soviet Union in two days than the U-2 reconnaissance aircraft had collected in two years of flights. Building on this success, the US reconnaissance program moved ahead rapidly, launching more than 100 reconnaissance satellites by 1972.⁴

Throughout this period, reconnaissance satellite technology and data were tightly controlled. When the US and the Soviet Union completed the first Strategic Arms Limitation Treaty in 1972, the agreement referred to verification by "national technical means." While this was understood by both parties to the treaty to refer to reconnaissance satellites, they deliberately chose not to publicly acknowledge the existence of these assets.⁵ Even the presence of the United States National Reconnaissance Office (NRO), the agency that developed remote sensing satellites, remained classified until 1992.⁶

The United States' high level of secrecy and reluctance to share technology and data extended even to allies. In 1973, Israeli officials requested access to US reconnaissance imagery in support of the Yom Kippur War. US officials responded that the information was not available due to damage to the satellite. While this may have been true, Israeli officials were not convinced and chose to proceed with Israel's own satellite reconnaissance program.⁷ Israel launched its first reconnaissance satellite, *Ofeq-1*, in 1988. This made Israel the fourth country in the world to develop a reconnaissance satellite, after the United States, the Soviet Union (1961), and China (1975).

The 1991 Persian Gulf War demonstrated continued limitations in US sharing of reconnaissance data with allies. In 1992, France requested US satellite imagery to support its efforts in the Gulf War. When the US declined to share the images, France started its own reconnaissance program.⁸ France's first reconnaissance satellite, *Helios 1A*, was launched in 1995, fol-

lowed by increasingly capable satellites in the same series. France was the fifth nation to develop a reconnaissance satellite. The data from this series was used to support independent French decision-making. A French military official stated in 2015 that it was because of Helios imagery that France declined to join the 2003 US invasion of Iraq, as France's independent assessment of this imagery contradicted US interpretations of intelligence at the time.⁹ See table 1 for inaugural satellite launch dates by country.

Table 1. Date of first reconnaissance satellite launch by country

Nation	First Reconnaissance Satellite
United States	1960
Soviet Union/Russia	1961
China	1975
Israel	1988
France	1995
Japan	2003
Germany	2006
India	2009
South Africa	2014
Turkey	2016
Italy	2017

While other factors, such as technical capability and prestige, likely impacted these decisions, US reticence to share its own reconnaissance data when requested also played a role in the Israeli and French development of independent reconnaissance satellite systems. Further, once these nations developed this technology, they were free to share the resulting information—or the technology itself—according to their own policies.

Unlike the US, France chose to undertake its satellite reconnaissance program as a cooperative effort. *Helios 1* was developed in partnership with Italy and Spain.¹⁰ Later Helios satellites incorporated Greece and Belgium into the partnership. In 2006, Germany developed its own reconnaissance satellite system, SAR-Lupe, with a radar instrument allowing the collection of information regardless of weather and lighting conditions. A cooperative treaty with France allows both nations to access data from both the Helios and SAR-Lupe satellites.¹¹ France has a similar agreement in place for access to data from Italy's dual-use COSMO-SkyMed constellation, launched in 2007 and 2008, which also carries radar instruments.¹² In 2017, Italy launched its first dedicated reconnaissance satellite, built by Israel Aerospace Industries.¹³

In addition to the significant degree of data sharing among European nations, Israel, France, and others have also proven to be much more willing than the US to export advanced satellite remote sensing technology. Despite a multiyear process that began in 2009 to reform export control regulations, remote sensing systems with military applications remain on the tightly controlled United States Munitions List.¹⁴ These systems include those with high spatial or spectral resolutions and many of those with radar remote-sensing characteristics. By contrast, allied nations spurred by the US to develop their own reconnaissance systems have shown a willingness to export this technology. In 2009, India launched its first reconnaissance satellite, the *Radar Imaging Satellite-2*, built by Israel Aerospace Industries. That same year, Turkey signed a contract with Thales Alenia Space of France and Italy's Telespazio to purchase a high-resolution imagery satellite, launched in 2016.

It is worth noting that, beginning in the 1980s, many countries—including the United States—promoted the growth of commercial remote-sensing companies capable of providing high-resolution imagery. The data sold by companies has proven valuable for national security and foreign policy uses.¹⁵ However, these companies remain highly regulated. Limitations are placed on the spatial resolution of this imagery to ensure it remains less precise than data provided by advanced military reconnaissance systems. Companies are often prohibited from selling data in particular geographic areas, to particular customers, or at particular times.¹⁶ While companies are regulated by the nation in which they reside, the US has also exerted “checkbook shutter control.” That is, it purchases all available imagery under an exclusive license so no one else can access it. The US thus has a way of wielding some level of control even over foreign commercial systems. While some countries may find that their national security needs can be met solely through commercially available satellite data, the continued limitations on access and the differences in capability differentiate them from nationally owned reconnaissance satellites.

As Nye and Owens suggested, by failing to adequately share data, the US had created an additional incentive for allies to develop their own systems sooner than they may have otherwise. Once that development had occurred, the US ceded not only its leverage as a data provider but also control over further proliferation of both the information and the underlying technology.

Global Navigation Satellite Systems

Limited US data sharing also acted as an incentive for independent allied development of global navigation satellite systems. The US Department of Defense (DOD) launched the first experimental navigation satellite, *TRANSIT 1A*, in 1959. The system used measurements of the Doppler shift in the satellite signal to determine a receiver's location on Earth. The DOD planned to use the system to allow accurate positioning of submarines carrying Polaris missiles. The system was declared operational in 1964. A second system, Timation (time/navigation), experimented with spacecraft carrying precise clocks, with an initial launch in 1967. This project evolved into the Global Positioning System (GPS), established in 1973. By 1978, four GPS Block 1 satellites were operational. Although the constellation would not be considered operational globally until 24 satellites were in orbit (which occurred in 1993), the system proved to have utility early on.¹⁷

The Soviet Union engaged in the development of a parallel system, the Global Navigation Satellite System (GLONASS), with 10 satellites in orbit by 1985. The constellation became fully operational in 1996 but was not maintained; it included fewer than 10 operational satellites, on average, between 1998 and 2006. The system returned to full operational capacity in 2010.¹⁸

In 1983, a civilian aircraft, Korean Airlines 007, strayed into Soviet airspace and was shot down by a Soviet fighter jet. Following this incident, President Reagan announced that the GPS signal would be made available for civilian use. However, the civilian signal would be less precise than the military signal—accurate to approximately 100 meters versus 10 meters for the military. The US government would also have a capability referred to as “selective availability” that would allow the civilian signal to be deliberately degraded or disabled. Despite these restrictions, civilian GPS receivers were in mass production by the late 1980s.¹⁹

In a 1992 communication to the European Parliament, the European Commission noted that although the US military currently made the GPS signal freely available for civil use, this arrangement could be halted at any time. Further, the civilian signal's accuracy was insufficient for use in the civil air navigation system, a highly desirable application.²⁰ In 1994, a European Parliament resolution officially called for establishing a European strategy for satellite navigation, and the Commission responded with a proposal for an independent European global navigation satellite system.²¹

In response to this movement and recognizing the growing commercial industry built on GPS, President Bill Clinton issued a directive stating

that the United States was committed to providing the GPS signal “on a continuous, worldwide basis, free of direct user fees.” The directive also stated that the US would discontinue the use of selective availability within a decade and that the government would advocate for the acceptance of GPS as the standard for international use.²² This was too little, too late for Europe, which continued ahead with plans to develop its independent Galileo global navigation satellite system.

In 2001, US deputy secretary of defense Paul Wolfowitz sent a letter to the defense ministers in selected EU countries. He argued that the planned European system could complicate US plans to modify and improve GPS due to potential interference of the Galileo signal with the upgraded US military signal on GPS. He further indicated that the civilian forum in which Galileo was being developed was insufficient to fully assess the security implications of the system.²³

European leaders did not respond well to this action. French president Jacques Chirac warned that Europeans risked “vassal status” if they abandoned the project. The European commissioner in charge of the project expressed frustration at “American pressure against the Galileo project” and the prospect of further delays.²⁴ The European Commission approved the next phase of development in 2002 and engaged in international cooperation, ensuring compatibility with the American GPS and Russian GLONASS systems. In 2016, the Galileo system reached initial operational status.²⁵ When Galileo becomes fully operational, it will be the fourth such constellation in the world, following the United States, Russia, and China. Once again, by refusing to make data available in a meaningful, reliable way, the United States added incentive for allies to create an independent system, and its efforts to dissuade such developments generated increasing tension.

Space Domain Awareness Systems

This pattern is being repeated once again for space situational awareness (SSA) systems—systems that track and analyze space objects to determine where they are, what they are, and where they are likely to be in the future.²⁶ The US has been tracking objects in space since the space age began with the 1957 launch of *Sputnik I*, and it has had an operational space surveillance system since 1958. The DOD worked with NASA, which also needed to track satellites, with both entities contributing observations to be cataloged by the DOD. In 1960, following the launch of the first Corona reconnaissance satellite, DOD officials determined that security concerns dictated withholding some data. The DOD began screening the catalog for

sensitive information before providing it to NASA, which then shared this information more broadly. This process, in which the DOD maintained a full tracking system while providing a subset of data to NASA for broader distribution, continued for more than 40 years.²⁷

In 2001, the US government released the *Report of the Commission to Assess United States National Security, Space Management and Organization*—more commonly known as the Rumsfeld Report after the commission chairman, Secretary of Defense Donald Rumsfeld. The report recognized the significant and growing dependence of the US military and economy on space assets and noted that this made space assets potentially attractive targets for adversaries. The report warned of a “Space Pearl Harbor” and emphasized the need to improve SSA. Space situational awareness is critical to avoiding unintentional collisions among satellites and other debris in space and detecting and attributing attacks on space assets.²⁸

In addition to the need for SSA data for military purposes, there was also a recognition that with the growth of commercial activity and increased civilian reliance on space assets, the US Air Force should provide warnings of threats to US or other friendly satellite operators. In 2000, a DOD memorandum directed the Air Force to study options for providing SSA support to commercial and foreign entities. The National Defense Authorization Act for Fiscal Year 2004 directed Air Force Space Command to implement a pilot program in this area.²⁹ The pilot program later became the operational SSA Sharing Program.

While the stated goal of the pilot program was to encourage international cooperation and transparency with foreign nations, the initial implementation fell short of expectations. The US Air Force maintained two catalogs—an internal high-accuracy catalog with detailed information on all tracked objects and the publicly accessible space track catalog with more basic information on a subset of space assets. The DOD routinely conducted conjunction analysis to determine the risk of a collision only for US military spacecraft, and the public catalog was inadequate to independently run this type of analysis. The limitations of this approach were demonstrated dramatically by the 2009 collision of an operational commercial Iridium communications satellite and a defunct Russian Cosmos satellite, which occurred with no advanced warning for Iridium operators.³⁰

Following the Iridium-Cosmos collision, the US began running conjunction analysis for all operational satellites and contacting satellite operators in the event of a potential collision. However, initial efforts struggled to balance the desire to work with satellite operators with the need to protect sensitive data. One Air Force analyst described early efforts at assisting

operators in planning collision avoidance maneuvers as “kind of like playing ‘Marco Polo.’”³¹

The US military has taken steps to substantially improve the situation since then. As of 2019, Strategic Command had signed agreements related to SSA services and data sharing with 19 nations; two international organizations; and more than 77 commercial satellite owners, operators, and launchers. These agreements allow higher-quality data to be shared more systematically.³² The military has also begun increasing the amount of data made available through its public catalog.³³ Further, recent years have seen the emergence of commercial SSA entities, particularly in the United States, that sell SSA data and analysis to domestic and foreign satellite operators.³⁴

However, there are still notable limitations to SSA data sharing. Even with recent improvements, the data provided in the public catalog remains insufficiently accurate to carry out conjunction analysis, and the US does not accept any liability for the information it shares.³⁵ Even when more accurate information or conjunction analyses are shared, the US does not provide insight into its data sources or algorithms, making it impossible for users to independently evaluate accuracy or conduct further analysis.³⁶

The United States reserves the right to deny participants access to SSA data and information without prior notice or explanation. Participants in the SSA data-sharing program are restricted from redistributing the data without explicit approval from the US. Furthermore, users note that while the data is currently provided free of charge, the US government provides no guarantee that this will continue to be the case in the future. Outside of these specific limitations, some partners remain generally uncomfortable relying on a program run by the US military as it may have different priorities and concerns than foreign, commercial, and civil users.³⁷

The slow development of data-sharing systems by the United States, combined with the continued limitations of those systems, has driven a number of allies to begin development of independent systems. In 2005, the European Commission convened a panel of space experts to report on security issues related to the European Space Policy. The group noted that while the United States was currently providing tracking data for free, “this situation could change in the near future, and the data already provided are not exhaustive or not be[ing] made available at the needed time.” It recommended the development of a European space surveillance capability as a high-priority activity.³⁸ The European Commission announced in 2008 that it would develop this capability, emphasizing Europe’s need

for political and technical autonomy.³⁹ In 2016, the European Union Space Surveillance Tracking system became operational.⁴⁰

A 2018 report by the Institute for Defense Analysis identified a lack of confidence in DOD-provided data as a key driver for many foreign and commercial entities developing independent capabilities. In interviews, officials cited the lack of transparency related to DOD data, particularly the lack of insight into processing methods, as a key source of concern. Others called attention to issues of accuracy and completeness of the data provided. South Korean government officials estimated that their country was receiving data for about only 40 percent of objects tracked by the DOD. In addition to Europe and South Korea, India, Canada, Australia, and Japan are among those developing or improving national SSA capabilities.⁴¹

Unexpected Benefits: Redundancy and Improved Capabilities

In each of the above cases, the United States had an information advantage based on superior technology, just as Nye and Owens suggested. While the US did make some data available to allies, its efforts fell short of allies' needs and expectations. In all three cases, allies directly referenced the lack of US data sharing as a factor in developing independent systems. The US choice to limit the sharing of data—versus using data sharing to provide the basis of coalition leadership and to maintain technological superiority—led to tensions between the United States and its allies and contributed to allies' decisions to develop independent systems.

From Nye and Owens's perspective, this approach may be viewed as a strategic failure on the part of the United States. However, the development of independent allied systems has ultimately benefited the US. As US reliance on space assets has increased, their vulnerability has become a growing concern. The 2018 *National Defense Strategy* recognized that new threats to military and civil use of space were emerging and called for investments to prioritize efforts to assure space capabilities.⁴² One of the widely agreed-upon methods for overcoming or deterring attacks on these assets is the development of redundant, resilient systems.

For example, given sufficient interoperability between the systems, if an adversary were to damage or disrupt GPS, the United States could switch to the Galileo signal. An attack on GPS would potentially have other ramifications, such as nuclear denotation detection, that would need to be dealt with in other ways. However, if the goal was to disable GPS, the ability to use Galileo should still be a deterrent. Knowing this, the adversary may determine that it is not worth attacking GPS in the first place. The same is true for redundant space reconnaissance and SSA systems.

From this perspective, allies' development of redundant military space systems may appreciably increase US national security. By engaging allies to build partnerships enabling the mutual sharing of information and technology, the US can reduce its vulnerability in these areas.

In addition to the benefits of resilience, cooperation and interoperability can improve performance. If the United States can negotiate gaining access to data from foreign reconnaissance systems, it will increase the volume of data available for analysis. Even without gaining regular access, the United States may reasonably assume that allies with mutual security concerns may be conducting surveillance and analysis with similar goals. Increasing the amount of data collected and the number of individuals and organizations analyzing this data reduces the risk that security threats will go undetected.

Coordinating navigation systems could be similarly beneficial. Receivers that can access the Galileo signal, in addition to GPS, will have more precise positioning capabilities. They will also be more likely to have access to a sufficient number of satellites for accurate positioning, even in rough terrain or urban canyons, and be more resistant to jamming or spoofing efforts. The United States and Europe have already begun to work toward this capability for military systems.

SSA technologies are primarily ground based, but the benefits of redundancy and improved performance are similar. The ability to accurately detect and attribute attacks on space assets, which relies on high-quality SSA data, is a crucial element in deterring such attacks. Just as for traditional reconnaissance data, the more space surveillance data that is collected and analyzed, the more likely it is that nefarious behavior will be detected and accurately attributed, thus improving deterrence.

While these examples focused on the military benefits of engaging allies in their development and operation of redundant systems, in the case of GPS and SSA, improved capabilities would also benefit civilian and commercial users of these systems.

Implications and Lessons Learned

Nye and Owens were not wrong when they recognized in 1996 that the nation able to lead in the information revolution would accrue power, and they correctly identified information sharing as an important source of leverage with allies. As was demonstrated in the cases of reconnaissance satellites, GPS, and SSA, they also correctly predicted that a lack of sharing would add an additional incentive for allies to attempt to match US

capabilities. What they failed to adequately account for was the important military benefit that can result from access to independent systems.

This benefit suggests that Nye and Owens's vision of an information umbrella must be updated. Rather than sharing data to maintain technological superiority, the United States should share its data to encourage partner contributions, interoperability, and resiliency. As Moltz identified, these attributes are the keys to twenty-first-century space power. The US should seek to be a coalition leader, just as Nye and Owens envisioned, but this coalition should aim to bring allies together to mutually share information in an "interoperable information umbrella."

Engaging with allies to encourage their technological development, rather than seeking to prevent it, is likely to generate stronger ties and reduce tensions. Acting as a leader in information exchange and interoperability also gives the US military greater flexibility in data-sharing decisions because allies are not entirely dependent on the United States. Thus, decisions to withhold some data have less of an adverse effect. Further, to the extent that data is shared, the United States can see concrete benefits as allies respond in kind, improving US military capabilities.

In the area of reconnaissance satellites, this stance could propel efforts to engage in more formal international coordination and data sharing with allies in Europe. The US would have multiple options for how to accomplish this. Rather than disclosing data from its most advanced, highly classified reconnaissance systems, it may opt to coordinate the development of jointly owned systems or to contribute data from a system specifically designed to complement allied capabilities.

For global navigation satellite systems (GNSS), cooperation and efforts to ensure interoperability with Europe's Galileo system are already well underway. However, it is worth noting that the US could have avoided much acrimony with its allies if this cooperative effort had begun a decade earlier. It may have a chance to do things differently by pursuing interoperability from the beginning if the United Kingdom moves forward with current plans to develop a GNSS.⁴³

Data sharing and engagement are perhaps most advanced for SSA. The US Space Command, reestablished in July 2019, has continued the efforts begun by US Strategic Command to pursue data-sharing agreements that enable a greater degree of information sharing with partners.⁴⁴ These agreements also provide the United States access to data sources from many different entities and create an opportunity to understand and address challenges of system and data interoperability. Some nations—such as Japan, Australia, and Canada—have identified interoperability with US

systems as a goal for developing SSA systems.⁴⁵ The United States should encourage other nations to follow a similar path and engage with more independent systems, such as those being developed in the European Union, to explore options for interoperability early on.

As noted above, decision-makers have many options concerning how to assimilate the factors discussed here. There is no one-size-fits-all solution for all technologies, at all times, with all potential partners. Prestige, technical capability, economics, varied strategic interests, and other factors will continue to influence whether and when nations choose to develop independent capabilities. The dynamics of the security dilemma may play a role as well, and decisions to share data could help to alleviate or exacerbate the situation. However, this factor would likely be more relevant to sharing that extends to US adversaries rather than to allies.⁴⁶ In any situation, the United States must carefully consider the potential risks of sharing data or coordinating on technical development. However, the potential benefits of information sharing and the pursuit of interoperability should not be overlooked.


The examples above suggest that when US decision-makers determine how much data they are willing to share, when, and with whom, they should heed Nye and Owens's warning that these decisions may impact allies' decisions to develop their own capabilities. Nye and Owens argue that greater data sharing could be used to extend the period of US technical superiority. The examples described here suggest that the effect they identify is present, but their argument misses a key point. As noted by Moltz, with respect to information technology, redundancy and interoperability are often more valuable to national security than technical superiority because they can increase capabilities and provide resilience to the entire system. Data sharing is a way to gain leverage with allies and build coalitions, and when combined with engagement to develop interoperable systems, these relationships can be even stronger.

Conclusion

We have entered the information age, and as predicted by Nye and Owens, and argued by Moltz, our conception of power must adjust to this new environment. Nye and Owens argued that the United States should create an information umbrella, sharing data from its superior information technologies with allies to generate leverage and preserve technological superiority. They predicted that if the United States failed to share its knowledge, other nations would be incentivized to match its capabilities. This effect was seen in the cases of reconnaissance satellites, GNSSs, and SSA.

In the case of reconnaissance satellite data, the United States refused offers to provide imagery despite direct requests from close allies during conflict situations. With respect to GPS, the US provided non-US military users with a significantly degraded signal and emphasized its right to further degrade or disable the signal at any time. Changes to these policies proved to be too little, too late. Similarly, while the US proactively put in place a system for sharing space situational awareness data with foreign entities, it provided relatively low-quality data and gave no commitment to long-term provision. Even as systems for sharing space surveillance data have improved over time, the US has shown no interest in making its full high-accuracy catalog, raw sensor data, or algorithms available to its allies.

In each of these cases, US reticence to share data resulted in tensions with its allies and, ultimately, contributed to incentives to develop independent allied systems. However, these developments had critical benefits that Nye and Owens did not foresee in their assessment. The independent systems provide redundancy and resilience that underlie deterrence and, when systems are made interoperable, can result in appreciable capability improvements. As noted by Moltz, these disaggregated systems and cooperative relationships offer a superior model for facing twenty-first-century challenges.

To account for this advantage, the US should seek to lead the creation of an interoperable information umbrella. In spearheading this international cooperative effort, the US would share data with its allies. However, it would do so as part of a reciprocal system in which allies are encouraged to develop systems that can contribute data while also improving the system's resiliency as a whole. As noted above, the specific pathways to pursue this effort will differ depending on the timing, technology, and set of partners involved. This strategy recognizes the unique opportunity of the information age to maximize US power: strengthening relationships with allies, increasing system resiliency, and improving military capabilities. 

Mariel Borowitz

Mariel Borowitz is an associate professor in the Sam Nunn School of International Affairs at Georgia Tech. Her research deals with international space policy issues, including international cooperation in satellite data-sharing policies and space security.

Notes

1. Joseph S. Nye and William A. Owens, "America's Information Edge," *Foreign Affairs* 75, no. 2 (1996): 20, <https://doi.org/10.2307/20047486>.
2. Nye and Owens, 20.

3. James Clay Moltz, "The Changing Dynamics of Twenty-First-Century Space Power," *Strategic Studies Quarterly* 13, no. 1 (Spring 2019): 66–94, <https://www.airuniversity.af.edu/>.
4. Robert L. Perry, *A History of Satellite Reconnaissance: The Perry Gambit & Hexagon Histories* (Chantilly, VA: Center for the Study of National Reconnaissance, 2012), <https://www.nro.gov/>.
5. Assistant Deputy Director for Plans and Policy, National Reconnaissance Office, to Col Von Ins, memorandum, subject: 156 Committee Recommendations, 12 November 1971, <https://www.nro.gov/>.
6. Bruce D. Berkowitz with Michael Suk, *The National Reconnaissance Office at 50 Years: A Brief History*, 2nd ed. (Chantilly, VA: Center for the Study of National Reconnaissance, 2018), <https://www.nro.gov/>.
7. E. L. Zorn, "Israel's Quest for Satellite Intelligence," *Space*, no. 1 (1991): 76.
8. Pierre Tran, "Space Intel Gives France Policy Independence," *Defense News*, 26 February 2015, <https://www.defensenews.com/>.
9. Peter B. de Selding, "Imagery Proliferation Has Diplomatic Cost for France," *Space News*, 8 July 2015, <https://spacenews.com/>.
10. Tran, "Space Intel."
11. Peter B. de Selding, "Germany's 2nd Military Radar Satellite Launched from Russia," *Space News*, 29 June 2004, <https://spacenews.com/>.
12. Peter B. de Selding, "French Helios 2B Spy Sat Sends Back First Test Images," *Space News*, 4 January 2010, <https://spacenews.com/>.
13. de Selding, "French Helios 2B"; and Jeff Foust, "IAI Sees Growing Demand for High-Resolution Imaging Smallsats," *Space News*, 6 September 2017, <https://spacenews.com/>.
14. US Department of Commerce, Bureau of Industry and Security, "Export Control Reform Spacecraft and Satellites," PowerPoint presentation, 14 November 2014, <http://bis.doc.gov/>.
15. Dana Kim, "The 'Democratization of Space' and the Increasing Effects of Commercial Satellite Imagery on Foreign Policy," *New Perspectives in Foreign Policy* 18 (Summer 2019): 35–38, <https://www.csis.org/>.
16. Ulrike Bohlmann and Alexander Soucek, "From 'Shutter Control' to 'Big Data': Trends in the Legal Treatment of Earth Observation Data," in *Satellite-Based Earth Observation: Trends and Challenges for Economy and Society*, eds. Christian Brünner et al. (Springer International Publishing: Springer, 2018), 185–96, <https://link.springer.com/book/10.1007/978-3-319-74805-4>; Michael R. Hoversten, "US National Security and Government Regulation of Commercial Remote Sensing from Outer Space," *Air Force Law Review* 50 (2001): 253; Sarah Scoles, "How the Government Controls Sensitive Satellite Data," *Wired*, 8 February 2018, <https://www.wired.com/>; B. Schmidt-Tedd and M. Kroymann, "Current Status and Recent Developments in German Remote Sensing Law," *Journal of Space Law* 34, no. 1 (2018): 97; and Thomas Gillon, "Regulating Remote Sensing Space Systems in Canada—New Legislation for a New Era," *Journal of Space Law* 34, no. 1 (2018): 19.
17. Norman Bonnor, "A Brief History of Global Navigation Satellite Systems," *Journal of Navigation* 65, no. 1 (January 2012): 1–14, <https://doi.org/10.1017/S0373463311000506>.

18. Peter B. de Selding, "Russia Pressing Ahead with Glonass Upgrades," *Space News*, 17 January 2012, <https://spacenews.com/>.
19. Bonnor, "Brief History."
20. Commission of the European Communities, *The European Community and Space: Challenges, Opportunities and New Actions*, Communication from the Commission to the Council and the European Parliament, COM (92) 360 final, Brussels, 23 September 1992, <http://aei.pitt.edu/5806/>.
21. Vincent Reillon, *Galileo: Overcoming Obstacles: History of EU Global Navigation Satellite Systems*, briefing (Brussels: European Parliamentary Research Service, April 2017), <http://www.europarl.europa.eu/>.
22. Office of Science and Technology Policy, National Security Council, "U.S. Global Positioning System Policy," fact sheet, 29 March 1996, <https://clintonwhitehouse2.archives.gov/>.
23. American Foreign Press, "US Warns EU about Galileo's Possible Military Conflicts," *Space Daily*, 18 December 2001, <https://www.spacedaily.com/>.
24. Barry James, "Washington Said to Fear Use of Galileo by Enemy in a War: U.S. Out of Line on Global Positioning, EU Says," *New York Times*, 19 December 2001, <https://www.nytimes.com/>.
25. Reillon, *Galileo*.
26. In October 2019, the US military began using the term "space domain awareness" to refer to this activity, emphasizing its view of space as a warfighting domain.
27. Rick W. Sturdevant, "From Satellite Tracking to Space Situational Awareness: The USAF and Space Surveillance, 1957–2007," *Air Power History* 55, no. 4 (Winter 2008): 4–23, <http://www.jstor.org/>.
28. *Commission to Assess United States National Security Space Management and Organization, Report of the Commission to Assess United States National Security Space Management and Organization* (Washington, DC: Commission, 2001), <http://www.europarl.europa.eu/>.
29. Sturdevant, "From Satellite Tracking to Space Situational Awareness."
30. Tiffany Chow, *Space Situational Awareness Sharing Program: An SWF Issue Brief* (Washington, DC: Secure World Foundation, 22 September 2011), <https://swfound.org/>.
31. Mariel Borowitz, "Strategic Implications of the Proliferation of Space Situational Awareness Technology and Information: Lessons Learned from the Remote Sensing Sector," *Space Policy* 47 (2019): 18–27, <https://doi.org/10.1016/j.spacepol.2018.05.002>.
32. US Strategic Command Public Affairs, "USSTRATCOM, Polish Space Agency Sign Agreement to Share Space Services, Data," US Strategic Command News, 11 April 2019, <https://www.stratcom.mil/>.
33. US Air Force Space Command Public Affairs, "USSTRATCOM Expands SSA Data on Space-Track.org," 10 October 2018, Air Force Space Command News, <https://www.afspc.af.mil/>.
34. Bhavya Lal et al., *Global Trends in Space Situational Awareness (SSA) and Space Traffic Management (STM)* (Washington, DC: Science & Technology Policy Institute, Institute for Defense Analysis, 2018), <https://iislweb.org/>.
35. Chow, *Space Situational Awareness*.
36. Lal et al., *Global Trends*.
37. Chow, *Space Situational Awareness*.
38. European Commission, *Report of the Panel of Experts on Space and Security* (Brussels: European Commission, 25 March 2005), 36, <https://www.statewatch.org/>.

39. Council of the European Union, "Council Resolution of 26 September 2008: Taking Forward the European Space Policy," *Official Journal of the European Union*, 26 September 2008, Publications Office of the EU, <https://op.europa.eu/>.
40. Regina Peldszus and Pascal Faucher, "European Space Surveillance and Tracking Support Framework," in *Handbook of Space Security: Policies, Applications and Programs*, ed. Kai-Uwe Schrogl (Berlin: Springer, 2020): 883–904, <https://link.springer.com/>.
41. Lal et al., *Global Trends*.
42. Department of Defense, *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge* (Washington, DC: Department of Defense, 2018), <https://dod.defense.gov/>.
43. Megan Gannon, "UK Ends Galileo Talks, Says It Will Explore a Homegrown Alternative," *Space News*, 4 December 2018, <https://spacenews.com/>.
44. US Space Command Public Affairs, "SPACECOM, Finnish Air Force Sign Memorandum of Understanding between Finland, US on Space Situational Awareness Cooperation," United States Space Command News, 4 November 2019, <https://www.spacecom.mil/>.
45. Lal et al., *Global Trends*.
46. Aleksander M. Lubojemski, "Satellites and the Security Dilemma," *Astropolitics* 17, no. 2 (2019): 127–40, <https://doi.org/10.1080/14777622.2019.1641689>; and Brad Townsend, "Strategic Choice and the Orbital Security Dilemma," *Strategic Studies Quarterly* 14, no. 1 (Spring 2020): 64–90, <https://www.airuniversity.af.edu/>.

Disclaimer and Copyright

The views and opinions in *SSQ* are those of the authors and are not officially sanctioned by any agency or department of the US government. This document and trademarks(s) contained herein are protected by law and provided for noncommercial use only. Any reproduction is subject to the Copyright Act of 1976 and applicable treaties of the United States. The authors retain all rights granted under 17 U.S.C. §106. Any reproduction requires author permission and a standard source credit line. Contact the *SSQ* editor for assistance: strategicstudiesquarterly@au.af.edu.