Dual Use Deception: How Technology Shapes Cooperation in International Relations

Jane Vaynman[a] and Tristan A. Volpe[b]*

[a]Department of Political Science, Temple University, Philadelphia, PA, USA
[b]Defense Analysis Department, Naval Postgraduate School, Monterey, CA, USA; Carnegie Endowment for International Peace, Washington, DC, USA
*Corresponding author. Email: tvolpe1@nps.edu

Abstract Almost all technology is dual use to some degree: it has both civilian and military applications. This feature creates a dilemma for cooperation. States can design arms control institutions to curtail costly competition over some military technology. But they also do not want to limit valuable civilian uses. How does the dual use nature of technology shape the prospects for cooperation? We argue that the duality of technology presents a challenge not by its very existence but rather through the ways it alters information constraints on the design of arms control institutions. We characterize variation in technology along two dual use dimensions: (1) the ease of distinguishing military from civilian uses; and (2) the degree of integration within military enterprises and the civilian economy. Distinguishability drives the level of monitoring needed to detect violations. When a weapon is indistinguishable from its civilian counterpart, states must improve detection though intelligence collection or intrusive inspections. Integration sharpens the costs of disclosing information to another state. For highly integrated technology, demonstrating compliance could expose information about other capabilities, increasing the security risks from espionage. Together, these dimensions generate expectations about the specific information problems states face as they try to devise agreements over various technologies. We introduce a new qualitative data set to assess both variables and their impact on cooperation across all modern armament technologies. The findings lend strong support for the theory. Efforts to control emerging technologies should consider how variation in the dual use attributes shapes this tension between detection and disclosure.

Almost all technology is dual use to some degree: it has both civilian and military applications. This attribute is the rule rather than the exception. Even the most lethal weapons often have peaceful counterparts or cousins in the civilian economy. The dual use nature of technology matters because it creates a dilemma for cooperation.

Consider the state of play in outer space, where nations are engaged in an arms race to build military platforms, notably anti-satellite weapons. By designing international institutions, in the form of new arms control agreements, states could curtail competition over expensive or dangerous weapons. But the same technology is integral to

International Organization 77, Summer 2023, pp. 599–632
 doi:10.1017/S0020818323000140

the civilian economy, with commercial actors also racing to field orbital systems for peaceful purposes. Unfortunately, many such civilian capabilities look like military armaments in space—even a benign net for clearing debris closely resembles a weapon for taking down satellites. This makes it hard for states to curb military applications without limiting themselves on the civilian side.

Beyond space, the dual use dilemma haunts cooperation over other technologies, such as cyber capabilities or biotechnology. States often fear that an adversary could exploit the peaceful uses of these technologies to cheat in plain sight, gaining a sudden military advantage. But this concern need not always doom efforts to craft arms control deals. States have used international institutions to control numerous military capabilities with civilian counterparts, from nuclear reactors and rockets to aircraft and naval vessels. Indeed, every modern arms control deal limits a military asset with some level of civil utility. This track record suggests that the overlap between civilian and military applications is not a singular attribute—it ranges across different technologies in ways that constrain or enable arms control agreements.

Unfortunately, there has been no systematic analysis of how variation in dual use technology shapes the prospects for cooperation in international relations. The general question of how technology affects international outcomes is a mainstay across the discipline.[1] Yet, many scholars narrowly focus on either the military or economic implications of technology. This bifurcated approach often overlooks the role that dual use technology plays as a general constraint on the design and viability of arms control institutions. At the same time, the duality of technology is a familiar consideration within select branches of security studies. In the nonproliferation realm, for example, cooperation seems difficult because states might build powerful weapons under the guise of peaceful nuclear, chemical, or biological programs. The dual use dilemma is clearly at work, but only as a perennial challenge for specific issues.[2] In this article we advance a broader concept of dual use that varies across all modern armament technologies. Our theoretical framework reveals how this foundational feature of technology affects whether and how states cooperate. However, we do not claim technology has a determinative effect on cooperation.[3] Many other factors play a role in arms control outcomes, and we use an "all else being equal" approach. We are interested in the distinct effects of a variable that scholars often underscore as important, without being clear on how.

We argue that the dual use nature of technology is best characterized along two dimensions: distinguishability and integration. *Distinguishability* is the relative ease of differentiating between a technology's military and civilian applications. Battleships are readily distinguishable from commercial cargo vessels, for example, but many military drones look the same as their civilian counterparts.

1. Horowitz 2020; Sechser, Narang, and Talmadge 2019.
2. Fuhrmann 2012; Koblentz 2009; Reppy 2006. Recent exceptions include Kardon and Leutert 2022; Pauly 2022.
3. See also Lieber 2008; Talmadge 2019.

Distinguishability affects the level of monitoring that states would need to verify compliance with arms control agreements. To cooperate on limits over indistinguishable technology, states must attain higher detection levels, either through better intelligence collection or through more intrusive inspections.

Integration reflects a technology's range and depth of use within military enterprises and the broader civilian economy. Niche technologies have low integration as they execute narrow, but sometimes significant, tasks. Long-range rockets, for instance, are limited to strategic strike and space launch missions, despite their pivotal role in power projection. By contrast, ubiquitous technologies, such as maritime vessels, are highly integrated into a wide range of military missions and civilian endeavors. Integration increases the security risks from arms control inspections. As a technology becomes more ubiquitous, it creates greater opportunities for inspectors to gather damaging information about armaments and assets beyond the scope of the deal. For example, inspection of shipyards to verify limits on battleships could pull back the veil of secrecy that protects other military and commercial vessels. A high risk of security damage due to information disclosure imposes a stronger constraint on the menu of monitoring options that states would be willing to accept as part of an arms control agreement.[4]

Together, these variables generate expectations about the specific information problems states face as they try to devise agreements over various technologies. The best prospects for arms control should emerge over distinguishable but niche technology. Here, the technology itself creates few constraints on cooperation—states can distinguish military violations from civilian activities without creating unacceptable security concerns. By contrast, indistinguishable technology with high integration should create a "dead zone" where both detection and disclosure problems doom the prospects for cooperation. Greater monitoring will be needed to verify compliance, but such measures risk revealing sensitive information about other military and economic capabilities. We also identify technologies with mixed dual use attributes in between these two extremes. In this range, the barriers to cooperation are more surmountable under some agreement forms, as states should only be confronted with either detection or disclosure problems from technology.

On the empirical front, we introduce a new qualitative data set that assesses both dual use dimensions and their impact on cooperation across an entire population of armament technologies. Instead of focusing on a small sample, we test our theory and demonstrate its generalizability by analyzing every technology in the case universe.[5] The literature lacks an accepted or even generally used list of weapon technologies, so developing this case universe in a systematic way is an empirical contribution of this article. We establish clear inclusion and exclusion rules to define the universe of cases around broad categories of weapons and weapon

4. On the use of international organizations to manage information disclosure, see Carnegie and Carson 2020.

5. Goertz 2017, 190–216.

platforms. Yet our categorization of technology is fine grained enough to differentiate major military capabilities. The result is a set of twenty-four technologies that states have used to arm themselves in the modern era. Our data set then uses case studies to measure each dual use variable and investigate how it shaped the information problems states have faced in designing arms control institutions.

Four patterns emerge from the evidence. First, *distinguishable and niche* technology creates minimal detection or disclosure barriers to cooperation. Arms control agreements over strategic capabilities, notably long-range ballistic missiles, land in this space. The distinguishability of this technology made it possible for states to rely on a larger set of options for verification, improving the prospects for cooperation.

Second, *indistinguishable and ubiquitous* technology creates severe information problems. Arms control agreements failed to emerge over almost every technology in this dead zone, from drones and cyber weapons to space capabilities. State negotiators confronted insurmountable detection and disclosure problems intrinsic to this type of technology, as illustrated by failed superpower efforts to curtail an arms race over anti-satellite weapons during the Cold War.

Third, *indistinguishable and niche* technology creates a severe but often surmountable detection constraint. In the nuclear realm, for example, the difficulty of distinguishing military from peaceful endeavors deepened the detection problem. But the niche nature of nuclear technology explains why states could accept intensive inspections in multilateral arms control agreements to improve detection: they faced manageable security risks from information disclosure.

Finally, *distinguishable and ubiquitous* technology creates a severe but manageable disclosure constraint. Agreements are limited in their use of intrusive monitoring, but detection needs are also lower because the military capabilities involved are relatively easy to differentiate from civilian equivalents. Many conventional military capabilities fall in this zone. To verify compliance in arms control deals over aircraft or naval vessels, for instance, states relied on national intelligence or monitoring with limited access based on geographic or physical boundaries.

Our research remedies problems of omission and underspecification in the three dominant accounts of how technology shapes cooperation. First, some contend that states face few incentives to limit military technology when it promises to provide them with specific advantages.[6] For example, a new technology could provide military superiority or offensive benefits for early adopters.[7] However, this argument struggles to explain the failure of cooperation when it seems beneficial from a defensive standpoint, such as limits over expensive or destabilizing weapons.

Second, states may favor arming over restraint when technology creates uncertainty about future applications. Competitive investments can be a prudent hedge

6. For the genesis of this argument, see Schelling and Halperin 1961. On its maturation as an international relations research program, see Glaser 2000.

7. Glaser 2010; Jervis 1978; Kydd 2000.

against vulnerability from unforeseen technological breakthroughs down the road.[8] But other scholars have shown that states can still reap the benefits of current cooperation by creating international institutions with provisions to provide flexibility in the face of uncertainty.[9] Further, technological uncertainty does not explain why states have struggled to create arms control around some well-understood capabilities. Because these explanations all narrowly focus on military characteristics, they overlook the economic incentives states have to avoid restrictions on a technology.

A third argument suggests that technology can saddle states with information problems. When capabilities are hard to observe, including when the line between peaceful and military uses is blurred, states will need greater transparency to detect cheating and so require onerous monitoring measures for an agreement.[10] This approach recognizes the challenge with dual use technology but oversimplifies it into a binary variable.[11] The lack of conceptual clarity means that, for example, the challenges to designing arms control institutions for armored vehicles seem similar to those regarding nuclear technology, because both are dual use. We are left with an intuitive sense that some capabilities are more dual use than others, but no framework specifying that variation or its implications. We expand on the information-oriented arguments by identifying how different dual use attributes shape the tension between detection and disclosure at the heart of arms control. Our findings show how future research can specify technology alongside other variables in accounting from arms control outcomes.

The following sections turn first to the theory and hypotheses. We then elaborate our research design and discuss the empirical results. The conclusion considers implications for the study of technology and cooperation, as well as policy efforts to manage artificial intelligence and other emerging technologies with new security institutions.

Theory

States can reap multiple benefits from arms control. Negotiated limitations can reduce resources spent on arms races, dampen incentives for conflict, and lower the risks of war. The literature has offered a long list of factors that are likely to either raise or lower the likelihood of security agreements, from relative power distributions and domestic politics to enforcement concerns. Our framework makes a *ceteris paribus* assumption. We avoid theorizing about other variables because our goal is to develop the logic of a separate effect for technology attributes. While political factors do affect arms control, omitting the independent impact of technology has hampered our understanding of international cooperation.

We think about the prospects for cooperation as characterized by constraints states face in designing arms control institutions. The prospects are poor when constraints

8. Green 2020; Lieber and Press 2017; Talmadge 2019.
9. Koremenos 2001; Kreps 2018; Kucik and Reinhardt 2008; Mantilla 2023; Williams 2019.
10. Abbott 1993; Debs and Monteiro 2014.
11. Chyba 2020; Coe and Vaynman 2020; Lin-Greenberg and Milonopoulos 2021.

narrow the range of cooperative options available in arms control negotiations. The prospects improve when there are fewer barriers to cooperation and the range of viable agreements expands. This view goes beyond a binary outcome of whether an agreement is likely to occur, and explores variation in the types of constraints states must address in a negotiated agreement to make cooperation possible. Our theory accounts for how technology itself can create distinct constraints on cooperation.

We focus on the logic of information problems. States often fail to cooperate because of a trade-off between transparency and security: agreements must provide enough information to detect violations, but not so much that they disclose deeper security vulnerabilities.[12] This trade-off implies that the tension between the detection and disclosure of information constrains cooperation in two ways. First, states need sufficient information to verify compliance with arms control agreements. They can use their intelligence tools or agree on cooperative monitoring rules to detect militarily significant violations. But gathering more information comes with costs. States must devote more resources to collecting information or allow foreign inspectors access to their territory. As these costs increase, the menu of acceptable monitoring options shrinks, thereby creating stronger detection constraints on arms control. Second, states also consider the degree to which cooperative monitoring creates security risks. Even minimal inspections might disclose damaging information, which creates a severe trade-off between transparency and security. Inspections to verify limits on specific weapons, for example, may reveal deeper vulnerabilities that enable an adversary to better attack other military forces. Alternatively, under a mild trade-off, the possible security damage from inspections would be more modest, so states face fewer disclosure-related constraints on cooperation.

The dual use nature of technology shapes both detection and disclosure constraints. First, the distinguishability of technology affects the level of monitoring needed to detect violations and verify compliance with an arms control deal. Second, the integration of technology sharpens the security risks from inspections. Our framework illuminates how inspecting highly integrated technology threatens to reveal sensitive military and industrial secrets beyond the scope of the agreement. We leverage these variables to generate hypotheses about the relationship between technology and the constraints on arms control agreements.

Distinguishability and the Detection Constraint

How does dual use technology impact the detection needs in arms control agreements? The notion that technology affects the information environment for states is a central tenet of offense-defense theory. According to this framework, cooperation is more likely when the nature of military technology makes it easier to distinguish offensive from defensive forces.[13] Greater differentiation draws clearer lines

12. On this mechanism, see Coe and Vaynman 2020.
13. Jervis 1978.

between weapon systems, which helps states negotiate limitations over offensive capabilities.[14] Traditional offense-defense theory provides a useful starting point: it draws our attention to how variation in military capabilities impacts the amount of information states need to make decisions about cooperation. But that military-focused approach was agnostic on how that information can change as technology blurs or sharpens the line between military and civilian applications. We therefore reformulate the concept of distinguishability to better capture the distinction between the military and civilian uses of technology.

In the dual use context, "distinguishability" refers to the relative ease of detecting whether a state is pursuing military or civilian activities.[15] Observation of highly distinguishable technologies helps states draw more confident estimates about the ultimate use of specific capabilities. High distinguishability also makes it harder for an adversary to practice deception because military assets cannot be easily disguised as civilian capabilities. Technologies with low distinguishability, on the other hand, facilitate deception—they obscure the true purpose of purportedly civilian applications of dual use capabilities.

We characterize distinguishability around four attributes. First, the *physical properties* of technology, such as its size or other detection signatures, set a concrete baseline. One reason biotechnology tends to have low distinguishability, for example, is that some of the lethal agents which have multiple peaceful and military uses are microscopic.[16] By contrast, warships are much easier to differentiate from civilian maritime vessels by their distinct size, shape, and construction material.

Second, the *development pathway* for technology affects the degree to which states can pursue military applications under the guise of peaceful aspirations. This calculus reflects the overlap or divergence between developing the technology for military or civilian purposes. Some technologies, for instance, use the same equipment and manufacturing techniques in both realms. But others follow distinct design and production processes compared to their military counterparts, making it costly to switch over from one production pathway to the other.

Third, *doctrine and deployment decisions* surrounding a particular technology can create patterns of observable behavior for civil and military uses. Despite drawing on the same technology, for instance, American and Soviet civilian space-launch centers with above-ground liquid-fueled rockets looked radically different from the military missile silos built underground at isolated ranges during the 1970s. Physical properties, development processes, and deployment patterns can also have implications for how costly it would be for a state to conceal a military capability. While it was once possible to make a metal warship look like a merchant vessel on a trade route, doing so required substantial modifications that degraded operational performance.

Finally, the *speed of conversion* captures how quickly an adversary could transform civilian capabilities into military assets. Faster conversion would make it

14. Glaser 2010, 75.
15. On the origins of this concept, see Volpe 2019.
16. Koblentz 2009, 64–67.

harder for others to observe development and deployment. Some technologies make it time consuming to convert production lines or repurpose platforms from civilian to military use. The longer this window of observation stays open, the easier it becomes for other states to detect an emerging military capability before it becomes operational.

We combine these attributes into low and high measures of distinguishability. As Table 1 summarizes, the attributes are distinct but can be interrelated in the context of specific technologies. For instance, the development of a technology over time may change the physical properties associated with its use in civilian versus military realms; and shifts in policy or doctrine can affect opportunities for conversion. From an analytical standpoint, it is helpful to consider the unique features of each attribute because one might be empirically more salient than another. When multiple attributes point in the same direction, gauging overall distinguishability is straightforward. It is also possible that a technology scores high on one attribute and low on others. In those cases, we assess the weight and relative importance of each attribute.

TABLE 1. *Distinguishability Attributes*

	Distinguishability	
Attributes	*Low*	*High*
Physical characteristics	Small/identical	Large/different
Development pathways	Overlapping	Divergent
Deployment patterns	Similar	Distinct
Conversion speed	Fast	Slow

Distinguishability matters for cooperation because it affects the level of monitoring needed to verify compliance. Indistinguishable technology increases the amount of information states must gather to differentiate permitted civilian from prohibited military activities. When technology blurs the line between military and civilian uses, deception is easier. A facility built for ostensibly civilian purposes, for example, could mask secret military activities. An agreement violation could therefore go undetected in plain sight.

States can surmount this detection problem by enhancing their intelligence capabilities or increasing inspector access for closer observation. But both approaches impose additional costs on cooperation, constraining the range of options that states will be willing to pursue. Unilateral intelligence collection is expensive and imperfect.[17] Even large intelligence investments may fail to yield adequate monitoring, especially when military violations are difficult to distinguish from peaceful

17. Zegart 2022.

behavior.[18] Inspections can help differentiate between prohibited and permitted activities. But this cooperative monitoring solution is predicated on allowing other states or international organizations access to territory, sensitive facilities, and even military forces. As indistinguishable technology drives up the need for better information to verify compliance, states must grapple with the ramifications of more intrusive or frequent arms control inspections. However, distinguishability is agnostic on the severity of these security risks—it affects only how much monitoring states will need to detect violations of a deal to control technology. We therefore turn to another attribute to understand how technology shapes security risks, and, in doing so, imposes a disclosure constraint on cooperation.

Integration and the Disclosure Constraint

The dual use nature of technology can sharpen the security risks from arms control inspections. We introduce a new concept, integration, to characterize how much damage could be caused by allowing inspectors to observe a particular military or civilian application of a technology. Integration reflects a technology's breadth of use within military enterprises and the civilian economy. Some technologies manifest little integration, as they perform few tasks in either realm. At the dawn of the space age, for example, satellites were limited to niche surveillance missions and select scientific endeavors. Other technologies offer more ubiquitous applications. Fixed-wing aircraft, for instance, have had many different military and commercial roles for well over a century. Greater integration within each realm increases the potential damage from information disclosure—primarily to military forces but also to the civilian economy.

Our concept of integration is based on the pervasiveness and marginal cost of technology. These two attributes come from economic research on "general-purpose technologies" that enjoy ubiquitous civilian use.[19] We repurpose each feature to better account for the degree to which technology is integrated within military enterprises and the civilian economy.

A technology's *pervasiveness* reflects its range and depth of use in each realm. Economists focus on technologies with broad commercial applications—the steam engine and the digital computer are paradigmatic examples.[20] We extend this logic to reflect variation in both the military and civilian uses of technology.[21] On the military side, ubiquitous weapon or platform technologies, such as conventional explosives or naval vessels, can be widely used to perform many different missions. By

18. Our theory holds changes in monitoring capabilities constant to understand the separate effects of distinguishability on the detection problem. Empirically, however, such capabilities do change over time independent of arms control needs. In measuring distinguishability, we consider the extent to which the outcome could be the result of changes in monitoring capabilities rather than distinguishability. See also Lin-Greenberg and Milonopoulos 2021.

19. Bresnahan and Trajtenberg 1995, 84.

20. Lipsey, Carlaw, and Bekar 2005, 97–98.

21. See also Ding and Dafoe 2023.

contrast, niche technologies execute a narrow range of missions. For example, until the mid-nineteenth century rifles were isolated to special military operations where range and accuracy were paramount. On the civilian side, technologies with ubiquitous applications can perform many peaceful tasks. Conventional explosives and maritime vessels, for instance, are used for a wide variety of commercial purposes, from industrial excavation with shaped charges to freight transportation on merchant ships. A niche technology has few peaceful applications in the civilian realm. The limited peaceful use of rifles for sport and game purposes is a long-standing case in point.

The *marginal cost* of a technology impacts its propensity for widespread adoption. Economists find that general-purpose technologies improve and become cheaper to use over time.[22] This idea translates seamlessly to the realm of both civilian and military innovation—the lower the per-unit cost of development and deployment, the easier it should be for actors to adopt the technology. The origins of the technology can also shape this cost function. Capabilities that begin life as commercial innovations tend to be cheaper than those born in the military realm because economic competition drives down development costs.[23] Related to costs, a technology with "spillover potential" means that government investment in military innovations is more appealing because of their eventual commercial benefits, or that private-sector innovation can be readily spun into military capabilities.[24] On the other hand, many other technologies offer complete solutions with little spillover effect on other capabilities. Table 2 summarizes these attributes.

TABLE 2. *Integration Attributes*

	Integration	
Attributes	*Low*	*High*
Range and variety of uses	Niche/isolated	Ubiquitous/pervasive
Marginal cost	Higher	Lower

We combine these attributes into high versus low measures of integration within military enterprises and the civilian economy. This allows us to categorize whether technology exhibits similar integration levels in both realms. Aerial drones offer a prime illustration on the high end. Intense commercial competition for smaller unarmed drones made many of these machines cheaper and easier to use relative to complex legacy platforms, which increased the value of further integrating the technology into new applications. The technology therefore became highly integrated

22. Jovanovic and Rousseau 2005, 3.
23. Horowitz 2010, 30–32.
24. Cowan and Foray 1995.

into a wide variety of military missions and civilian industries over time. On the low end, nuclear technology is emblematic of a significant but niche capability. Atomic weapons and energy assets can have major strategic and economic effects. But the expensive technology often ends up sequestered away from other capabilities to perform select military missions or peaceful functions.

The levels of military and civilian integration need not always covary in this fashion. A technology can have many uses in one realm but only niche applications in the other. Some technologies, such as artillery and armored vehicles, are highly integrated into military enterprises but occupy niche roles in the civilian economy—avalanche control and secure transportation, respectively. Other technologies, notably chemical and biological warfare agents, are isolated to specialized military units with narrow missions. Yet the peaceful cousins of these niche weapons enjoy ubiquitous civilian use: the chemical and biotechnology industries are woven into many sectors of the global economy. Specifying separate levels of military and civilian integration allows us to explore the effects of each on the information disclosure problem.

Integration shapes a major constraint on cooperation: it increases the security risks states face from granting inspectors access to observe a particular weapon or facility. The problem with highly integrated technology is that it enables espionage: allowing observation of a specific capability to verify limits on weapons risks revealing broader vulnerabilities.[25] Inspections are therefore more likely to disclose damaging information about military forces and economic assets beyond the scope of the agreement.[26] We therefore consider how integration within each realm shapes this disclosure problem.

When observing a technology with high military integration, inspectors may be able to collect information that reveals vulnerabilities in other military capabilities beyond the arms control deal. First, there could be other assets that rely on similar technology. Inspection of a specific subclass of aerial drones, for example, could disclose weak points in other military drones. The more integrated the technology becomes within military enterprises, the larger that "other" category is likely to be.[27]

The second threat comes from physical colocation. Highly integrated technology tends to be present in numerous locations, deployed near other capabilities, and used in many missions. This means that observation of such a weapon or platform risks exposing information about other military systems that are also located or operated with that technology.[28] By contrast, isolated technology creates natural firebreaks or moats around the capabilities being monitored as part of an agreement. Inspecting an atomic energy program, for instance, provides little insight into a state's capacity to field force beyond the nuclear realm. Espionage is still a

25. For similar arguments about discrete technologies, see Acton 2018; Gartzke and Lindsay 2015.
26. See also Carnegie and Carson 2020.
27. Schneider 2019.
28. Acton 2018.

concern, but observers will find it harder to use the technology as an avenue to expose broader military vulnerabilities.[29]

Inspecting the civilian applications of technology with high military integration also threatens to reveal dangerous information about latency—a state's capacity to field military forces in the future.[30] Consider an agreement to limit armed drones. Inspections of civilian drone factories could help verify that these ostensibly peaceful facilities were not being used as cover to build armed drones in secret. But the highly integrated nature of the technology means that even commercial inspections risk illuminating the deeper production base for military drones beyond just the armed platforms in the agreement. This information can be fed back into an adversary's targeting plans to destroy civilian facilities capable of military production in wartime. Or it can be used in peacetime to increase the attack surface for sabotage.[31] These security risks to military forces can be anticipated, which leads states to be wary of letting others monitor technology with high military integration.[32]

The integration of technology into the civilian realm creates concerns about economic damage from industrial espionage. States want to protect their domestic industries from observation that could benefit foreign competitors and enable adversaries to accumulate economic power.[33] As a technology becomes more widely used in the economy, it may enable inspectors to uncover trade secrets about a wider range of commercial products. In the example of drone technology, inspecting a civilian factory to confirm limits on armed drones could expose details of the design and manufacture of advanced power systems for valuable commercial drones. An adversary could funnel this proprietary information back into its industrial base to gain an edge in economic competition.[34] Beyond the cost to the monitored state's economy, industrial espionage can morph into a security risk if helps the adversary become more powerful. Allowing inspection of technology with high civilian integration therefore increases the potential for economic damage and power shifts.

In sum, integration constrains the cooperative monitoring options available to states because it increases the degree to which information disclosure could expose military or economic secrets. Whereas the detection problem drove the need for more information to manage fears of cheating, this disclosure challenge can arise even when states seek to demonstrate compliance with an arms control deal. We assume governments care most about protecting their military forces, followed closely by enhancing economic power. As higher military integration makes this primary security risk more severe, states are likely to reject intrusive inspections. We also expect states to factor in the economic damage from allowing an adversary to inspect highly integrated civilian technology.

29. On incentives to conceal military capabilities, see Green and Long 2020; Lindsey 2015.
30. Volpe 2023.
31. Rovner 2020.
32. Matovski 2020.
33. Carnegie and Carson 2020.
34. On the limits of industrial espionage, see Gilli and Gilli 2019.

Outcomes and Hypotheses

We combine the implications from the two dual use dimensions to generate four hypotheses about how technology shapes the constraints that states face in designing arms control institutions (summarized in Table 3).

TABLE 3. *How Technology Shapes Information Constraints on Cooperation*

		Distinguishability	
		High	*Low*
Integration	*Low*	Permissive zone (best prospects—H1) • Minimal detection or disclosure constraints • Additional monitoring not necessary to detect military violations from civilian uses • Monitoring less likely to disclose damaging information • Dual use nature of technology does not itself narrow range of viable arms control options	Detection constraint (modest prospects—H3) • Severe but surmountable detection constraint • More information needed to verify compliance • Niche technology creates fewer security risks from information disclosure • Dual use nature of technology leads states to pursue intrusive inspections over narrow technology subset
	High	Disclosure constraint (modest prospects—H4) • Severe but manageable disclosure constraint • Military violations easy to distinguish from permitted civilian uses • Integration creates high security risks from monitoring • Dual use nature of technology leads states to limit damage from monitoring via unilateral collection or restricted inspections	Dead zone (worst prospects—H2) • Severe detection and disclosure constraints • Greater monitoring measures needed to verify compliance • But high integration increases the potential damage from monitoring • Dual use nature of technology creates a dead zone for cooperation where states reject most arms control options

First, we expect the best prospects for arms control to emerge over distinguishable and niche technology. This type of technology should create minimal detection or disclosure constraints on negotiating arms control agreements. There is likely no need for additional monitoring to differentiate dual use applications—civilian activities should be easy to discern from military ones which could constitute violations. Whatever monitoring states see as necessary likely creates relatively lower security risks because the technology occupies a niche role with limited uses. Information gained from monitoring either civilian or military applications should not disclose damaging information about other capabilities.

H1: Best prospects for cooperation: niche and distinguishable technology are likely to create few detection or disclosure constraints on arms control agreements.

Second, the prospects for cooperation are likely to be the worst for indistinguishable and integrated technology. Here, the technology should create major detection

and disclosure constraints on cooperation. By blurring the distinction between military and civilian applications, the technology increases the need for more transparency to discern whether a particular activity is permitted or prohibited. But greater monitoring comes with severe security risks. High integration increases the damage states could incur from intrusive inspections because observing compliance in one area is likely to reveal sensitive information in another. As a result, there will be few or even no options where the security risks posed by an agreement do not outweigh its benefits.

H2: Worst prospects for cooperation: integrated and indistinguishable technology are likely to create a dead zone where severe detection and disclosure constraints doom arms control agreements.

Third, the prospects for cooperation over indistinguishable and niche technology are likely to be modest. This mix of dual use attributes should create a situation where states face a severe but surmountable detection constraint. We expect cooperation efforts to focus on subsets of the indistinguishable technology where reliable options exist for monitoring narrow distinctions between allowable and banned applications. Intrusive inspections will likely be necessary to verify compliance, but the lower security risks from observing niche technology should make states more comfortable with accepting those provisions as part of a deal.

H3: Modest prospects for cooperation: niche and indistinguishable technology should sharpen the detection constraint but enable cooperative monitoring in arms control agreements. States are likely to pursue intrusive inspection policies over a narrow range of activities.

Finally, distinguishable technology with high integration is likely to create a severe but manageable disclosure constraint on cooperation. The prospects for cooperation should be modest. Additional monitoring measures are unlikely to be necessary to differentiate between military and peaceful applications of the technology. Instead, the main barrier to cooperation should stem from concerns about the security risks—observation of the technology could disclose sensitive information about broader military forces and economic assets. We expect to see agreements contain features to protect states from this disclosure damage, either through reliance on unilateral intelligence collection or through careful restrictions on the intrusiveness of inspections, such as limits on their timing, extent, or geographic location.

H4: Modest prospects for cooperation: distinguishable and integrated technology should deepen the disclosure problem but dampen the dual use detection challenge. States are likely to pursue policies where the security risks from monitoring can be managed by safeguarding sensitive information or restricting the intrusiveness of inspections.

Research Design

We introduce a new qualitative data set that assesses both dual use dimensions and their impact on cooperation across all modern armament technologies. Instead of selecting sample cases from a larger population, our research strategy tests the theory by evaluating every technology within our case universe. Constructing a comprehensive data set demonstrates the generalizability of our claims across technologies. However, there is no consensus in the literature on a complete list of military technologies. We therefore establish a new universe of technology cases around clear inclusion and exclusion rules.[35]

Our case universe includes every technology that states have used to arm themselves with distinct weapons or weapon platforms in the modern era. This inclusion rule reflects the arms control phenomenon: state efforts to negotiate controls over the possession or use of military armaments.[36] A *weapon* is an object used to inflict injury or damage on enemy personnel or materiel. The term encompasses a range of capabilities with discrete damage effects, from conventional explosives to network attack tools. A *weapon platform* is a combination of one or more weapons with a vehicle or delivery system that can reach enemy targets. Thus, naval vessels and rockets can be platforms for hosting or delivering various weapons.

We exclude technologies that can be neither stand-alone weapons nor weapon platforms. This exclusion rule removes from our universe four types of technologies with military applications: (1) technologies that can constitute only a *component* of larger weapon or platform systems, such as a microprocessor or fuel pump in a rocket; (2) technologies that *enable* or *enhance* the performance of stand-alone armaments, such electricity and propulsion or stealth measures; (3) technologies that can perform only *support* or *logistics* functions, such as communication and cryptologic capabilities; and (4) the *means of production,* such as industrial manufacturing techniques. States may have other incentives to create international governance rules regarding such technologies—such as optimizing international trade—but these lie beyond our focus on managing the cost and risks of military armaments.

Scoping the universe around arms technology also guards against biasing the results in favor of our theory. Relaxing the exclusion rule would allow a case universe with even stronger support for several key hypotheses. Most of the excluded technologies would be coded as indistinguishable and highly integrated. Since there have been no international agreements to limit them, this larger universe of cases would seemingly lend significant support for our expectation about the dim prospects for cooperation in the dead zone (H2). While the nature of technology may indeed play some role in hindering international agreements, in these cases the benefits from mutual restraint are low, which creates few incentives for cooperation in the first place.

35. Goertz 2017, 190–216.
36. On this canonical definition, see Schelling and Halperin 1961, 3.

We leverage multiple studies to identify the largest possible candidate pool for inclusion in our case universe (the online appendix reviews these data). We also use the full text of every arms control agreement from 1816 to 2010 to check that our universe includes all capabilities limited under successful cooperation efforts. Histories of failed negotiations identify technologies over which agreements did not occur. Finally, we draw boundaries around technology categories based on the features that make each weapon or weapon platform unique. In cases where the technology is open to multiple definitions, we also consider whether different categorizations would change the coding of dual use attributes.

To measure the independent variables, we analyze the observable features for distinguishability and integration across the entire universe of technology cases, paying attention to any within-case variation over time. For distinguishability, we weigh the relative importance of each attribute to determine low versus high scores. For integration, we conduct separate assessments of the technology's relative ubiquity within military and civilian realms. The appendix provides a codebook with criteria to generate overall grades in a standardized manner.

To measure the dependent variable, we examine indicators of constraints states faced in designing arms control institutions. The success or failure of efforts to negotiate limits over arms provides a useful starting point, so we identify cases where agreements were signed or considered but ultimately failed. We also observe whether detection and disclosure problems shaped the arms control options available to states. For episodes where an agreement was signed, we identify the features included in the agreement, with attention on the measures for monitoring compliance and the scope of controls, as well as any negotiation details that point to technology-based constraints.[37] For unsuccessful episodes, we look at negotiations among states and internal deliberations to determine what role, if any, the constraints from technology played. Finally, technology is not the only factor affecting the design and likelihood of arms control. To deal with this equifinality issue, we identify dominant explanations and explain how our variables provide a more complete understanding of agreement outcomes, features, or negotiation issues.

Empirical Results

Table 4 summarizes our findings on how variation in the dual use nature of technology shapes the prospects for cooperation—the appendix contains full case studies on

37. To avoid selection bias, we test our hypotheses across all arms control agreements that emerge from our technology scoping condition. Our dependent variable therefore groups together several agreements that in other work are sometimes considered under different types of arms control, such as agreements where states agree to limit weapons to gain benefits from lower risk or reduced arms spending; postwar restraints imposed on a defeated power or other asymmetric deals where one side gains more than the other; and multilateral export controls designed to manage the diffusion of armaments by regulating technology transfers. The appendix considers how each agreement type affects theory evaluation.

TABLE 4. *Dual Use Technology Attributes and Arms Control Outcomes*

Technology (time period)	*Distinguishability*	*Integration (mil./civ.)*	*Outcome*	*Theory support*
Permissive Zone (H1):				
Rockets (1970–2020)	High	Low	Agreements with a mix of verification measures	Strong
Space (1957–1970)	High	Low	Agreement with unilateral collection methods	Strong
Dead Zone (H2):				
Biological (1953–2020)	Low	Low/high	Agreement but no verification protocols	Moderate
Cyber (1969–2020)	Low	High	Consideration but no agreement	Strong
Drones (2006–2020)	Low	High	Consideration but no agreements	Strong
Motor vehicles (1885–2020)	Low	High	No agreements	Strong
Space (1970–2020)	Low	High	Consideration but no agreements	Strong
Detection Constraint Zone (H3):				
Biological (1915–1953)	Low	Low	Agreement over narrow scope of activities	Strong
Chemical (1850–2020)	Low	Low/high	Agreement with intrusive verification regime	Strong
Firearms (1520–1840)	Low	Low	No agreements	Neutral
Hypersonic vehicles (1981–2020)	Low	Low	No agreements	Neutral
Rockets (1944–1970)	Low	Low	Deals considered but rejected on detection grounds	Strong
Nuclear (1945–2020)	Low	Low	Agreement with intrusive verification regime	Strong
Disclosure Constraint Zone (H4):				
Air defense (1940–2020)	High	High	Agreements with unilateral collection/inspection limits	Strong
Fixed-wing aircraft (1903–2020)	High	High	Agreements with unilateral collection/inspection limits	Strong
Rotary-wing aircraft (1942–2020)	High	High	Agreements with unilateral collection/inspection limits	Strong
Dirigible airship (1900–2020)	High	Low/high	Agreement imposed on defeated power	Neutral
Armored vehicles (1914–2020)	High	High/low	Agreements with unilateral collection/inspection limits	Strong
Artillery (1897–2020)	High	High/low	Agreements with unilateral collection/inspection limits	Strong
Conventional explosives (1847–2020)	High	High	Agreements with unilateral collection methods	Strong
Cruise missiles (1944–2020)	High	High/low	Agreements with unilateral collection/inspection limits	Strong
Drones (1982–2006)	High	High/low	Agreement with unilateral collection methods	Strong
Firearms (1840–2020)	High	High/low	Agreements with unilateral collection methods	Strong
Lasers (1982–2020)	High	High	Agreements with unilateral collection methods	Strong
Machine guns (1885–2020)	High	High/low	Agreements with unilateral collection methods	Strong
Maritime vessels (1869–2020)	High	High	Agreements with unilateral collection methods	Strong

Continued

TABLE 4. *Continued*

Technology (time period)	*Distinguishability*	*Integration (mil./civ.)*	*Outcome*	*Theory support*
Railcars (1914–1945)	High	High	Agreement imposed on defeated power	Neutral
Submarines (1866–2020)	High	High/low	Agreements with unilateral collection/inspection limits	Strong
Torpedoes (1871–2020)	High	High/low	Agreements imposed on defeated powers	Neutral

all twenty-nine episodes. We structure our analysis of these results around the four expected outcomes from Table 3. This enables us to assess the degree of empirical support for our hypotheses while considering other common accounts of arms control.

H1: Technology creates few detection or disclosure constraints

To assess this hypothesis, we examine efforts to control highly distinguishable arms technology with low levels of integration. Two cases in our universe exhibit both dual use attributes: (1) rockets (1970–2020), specifically intercontinental ballistic missiles (ICBMs) and space launch vehicles (SLVs), moved into this permissive zone as the technology grew more distinguishable; and (2) space technology (1957–1970), including satellites and orbital weapons, enjoyed an initial period in this zone before becoming indistinguishable and ubiquitous as the technology evolved.

In line with our expectations, the superpowers reached agreements with various monitoring provisions to limit the military uses of rocket and space technology. We focus on the rocket case because scholars have identified several other factors responsible for the success of arms control in the 1970s. The superpowers had mutual incentives to manage nuclear risks in the wake of the 1962 Cuban missile crisis, especially as both nations achieved parity in strategic forces.[38] These features certainly made arms control more desirable. But they cannot explain the information problems that doomed initial arms control efforts in the 1960s. Recent research argues that improvements in satellite surveillance made deals more viable by the 1970s.[39] Indeed, the superpowers could rely on these platforms to better monitor compliance. However, our results indicate that a shift in distinguishability occurred independent of improvements in monitoring technology, which effectively eliminated the dual use issue in strategic arms control negotiations.

In 1964, the superpowers attempted to negotiate a freeze on ballistic missiles. During this period, long-range rockets exhibited low integration because the

38. Gavin 2012; Green 2020; Maurer 2022.
39. Bateman 2022; Coe and Vaynman 2020, 352–53; Kalic 2012.

sophisticated technology played a narrow but significant role in placing payloads into orbit or delivering strategic warheads. Yet the effort failed, in large part because rocket technology was still plagued by dual use indistinguishability. The recent introduction of reconnaissance satellites enabled the superpowers to observe rocket capabilities; a key US National Intelligence Estimate (NIE) from 1962 revealed that "the major facilities involved in the Soviet space [launch] program have been identified."[40] But differentiating these civilian capabilities from military ICBMs presented a major challenge: "the USSR's space program has been closely linked to its military," and "the two programs have used the same boosters and launching facilities, and are mutually supporting in other respects as well."[41] This created an insurmountable detection challenge in negotiations. The Americans called for extensive on-site inspections of both military ICBM *and* civilian SLV facilities to verify compliance with its missile freeze proposal.[42] The Soviets rejected these inspection provisions, and the discussions ended in failure.

In the early 1970s, however, military ICBMs became more distinguishable from civilian SLVs. The design and especially the deployment patterns of military and civilian rockets started to differ. SLVs became larger to lift heavier payloads into space, continued to rely on liquid fuel, and were launched from well-known sites with extensive support infrastructure.[43] Earlier, both kinds of rockets had been launched from similar-looking above-ground launch pads. But by the late 1960s ICBMs started to be deployed in hardened silos (and eventually on purely military mobile launchers). US officials closely tracked this shift in Soviet missile dispersion.[44] Integration also remained low, as SLVs and ICBMs continued to perform the same limited set of important functions at high cost.[45]

This shift in distinguishability meant that the superpowers no longer faced detection challenges related to the dual use nature of rocket technology. One notable indicator of this change comes from a declassified 1971 NIE on Soviet rocket launch capabilities. In contrast to descriptions in earlier estimates, the US intelligence community could now easily separate ICBM from SLV capabilities. This had little to do with improvements in US reconnaissance satellites. Instead, the NIE explicitly focused on the observable physical differences and diverging development pathways between Soviet ICBMs and SLVs: carrying out more "complicated" space exploration missions required the Soviets to "advance their technology to a higher level" by fielding distinct booster systems and launch facilities apart from the ICBM

40. Central Intelligence Agency, "The Soviet Space Program," NIE no. 11-1-62, 5 December 1962. National Security Archive (NSA).

41. Ibid.

42. McGeorge Bundy, "A Missile Launcher Freeze Proposal for the President's State of the Union Message," Memorandum for the President, 28 December 1965. National Archives at College Park, MD, record group 59 PolMil.

43. Burrows 1999.

44. Department of State, "Recent Developments in Strategic Forces," 31 December 1966, Foreign Relations of the United States (FRUS), 1964–68, vol. X, doc. 163.

45. Burrows 1999, 206–209; Early 2014.

force.[46] By the time of the SALT I and SALT II negotiations in the 1970s, the US stopped demanding inspections, which created greater bargaining room for both sides to achieve foundational limits over ICBMs.[47] Subsequent deals, such as the Strategic Arms Reduction Treaty (START), Intermediate-Range Nuclear Forces (INF) treaty, and New START treaty incorporated inspections of specific military assets. But the dual use detection problem no longer haunted these negotiations.

H2: Technology creates a dead zone with severe detection and disclosure constraints

We assess this hypothesis by examining efforts to control indistinguishable armament technologies with high levels of integration. Our universe contains five cases with these attributes: (1) cyber weapons (1969–2020); (2) drones (2006–2020); (3) motor vehicles (1885–2020); (4) biotechnology (1953–2020); and (5) outer-space technology (1970–2020). Despite numerous efforts to negotiate limits, arms control agreements failed to emerge over almost all these technologies. Even the sole exception—the Biological Weapons Convention—supports our expectations, because it had major verification problems that rendered it flawed as a cooperative institution.[48] Consistent with H2, we find that the dual use nature of each technology created severe detection and disclosure constraints on cooperation.

The evolution of space-based technology, primarily satellites and other orbital platforms such as spacecraft, allows us to trace out how variation in distinguishability and integration can doom the prospects for arms control. There have been no limits on building weapons in space since the Outer Space Treaty was signed in 1967. The absence of new agreements was not for lack of trying. During the Cold War, the superpowers both recognized that an arms race over anti-satellite (ASAT) weapons could increase the risk of conflict. Yet negotiations to curtail ASAT capabilities failed in 1978–79, in 1981–82, and again in 1987–89.[49] Traditional theories of arms control struggle to explain why the superpowers were unable to reap mutual benefits by banning this dangerous class of weapons. Some scholars account for this failure by bringing in factors on the nature of the US–Soviet relationship, notably the end of détente in 1979 coupled with renewed fears about maintaining the nuclear stalemate.[50] Yet our results indicate that changes in both dual use dimensions of space technology during the 1970s plagued every ASAT negotiation with an insurmountable verification problem.

When space capabilities debuted in the late 1950s with the Sputnik and Explorer satellites, the technology enjoyed a brief period of high distinguishability and low integration. Early military and civilian space capabilities exhibited distinct physical

46. Central Intelligence Agency, "The Soviet Space Program," NIE no. 11-1-71, 1971. NSA.
47. Bunn 1992, 106–108.
48. Koblentz 2009, 53–105.
49. Bateman 2022.
50. Green 2020; Moltz 2008.

features while following divergent development pathways and deployment patterns to achieve different goals.[51] Space systems had also not yet become ubiquitous. The rudimentary technology could perform only a limited range of high-value military and prestigious civilian functions. Analysis of declassified US intelligence products suggests that the Americans were quite successful in identifying the purposes of Soviet satellites. These documents express little concern that US intelligence agencies would have a hard time differentiating between scientific satellites and those armed with strategic weapons.[52] As one report about distinguishing Soviet "bombs in orbit" concluded in 1966, "it would be extremely difficult to conceal such a program."[53] This level of distinguishability appeared to shape superpower expectations about verifying a ban on the placement of strategic weapons on orbital platforms—the Outer Space Treaty did not include verification provisions. Instead, US officials determined that they could rely on "substantial" national intelligence capabilities to distinguish benign Soviet satellites from strategic weapon platforms in outer space.[54]

In the early 1970s, however, advances in space technology made it harder to distinguish between military and civilian uses. American and Soviet satellites became more capable of performing both military or peaceful functions along similar orbital routes.[55] Even more worrisome, after the Apollo era ended, the focus of manned spaceflight turned toward missions aboard space stations, such as Salyut 1–7 (1971–86), Skylab (1973–79), Mir (1986–2001), and the Space Shuttle (1981–2011).[56] Since these civilian platforms could perform many different maneuverable rendezvous operations in space, it became harder to observe possible military uses. For example, the same spacecraft could dock with a satellite to repair it or to sabotage it. A 1982 CIA assessment concluded the ostensibly peaceful Mir space station would give the Soviet military cover "to pursue research in ASW [antisubmarine warfare], ASAT, early warning, and other important defensive and offensive missions."[57] The conversion speed from civilian to military capabilities also increased, as such platforms could be rapidly turned into orbital ASAT weapons. The Reagan administration worried that the Soviets could destroy American spacecraft "under the guise" of peaceful "space rendezvous and docking operations."[58] The Soviets similarly feared that the US Space Shuttle could be converted to drop a nuclear weapon on Moscow or attack their satellites.[59]

51. The appendix details each attribute.
52. Richelson 2015.
53. As quoted in Paine 2018.
54. Central Intelligence Agency, "Draft Recommendations Respecting US Approach to a Separate Arms Control Measure for Outer Space," no date, 12–13. CIA Reading Room.
55. Stares 1987.
56. Burrows 1999.
57. Central Intelligence Agency, "Outlook for Rapid Expansion of Soviet Space Programs Through 1986," Intelligence Assessment, October 1982, 12. CIA Reading Room.
58. Presidential Report to Congress, "US Policy on ASAT Arms Control," 31 March 1984. Government Printing Office.
59. Hendrickx and Day 2020.

Space technology also started to become highly integrated within both the military and civilian realms in the 1970s. On the military side, the range and variety of uses for orbital platforms expanded far beyond niche applications in the strategic nuclear realm.[60] The United States harnessed satellites to support conventional military forces in a wider variety of functions, notably precision strike and surveillance.[61] According to a CIA assessment from 1982, the Soviet military had become "increasingly dependent upon the new [space] systems for intelligence collection, navigation support, and maintaining order-of-battle and targeting data."[62] On the civilian side, space capabilities became ubiquitous as the emergence of commercial satellite services ended the government monopoly on orbital platforms.[63] By the 1980s, commercial satellites were being used in many economic sectors, from shipping and logistics to geodesic survey. The cost of space systems remained high in absolute terms, especially for bespoke satellites or advanced spacecraft. However, the rise of commercial services lowered the cost of accessing and even possessing satellites.[64]

The archival record shows that American and Soviet negotiators confronted serious detection and disclosure problems as they attempted to ban ASAT weapons in the later Cold War. In 1978, the Carter administration set out to "seek a verifiable ban on anti-satellite capabilities" as part of its official space policy.[65] In developing this position, senior US officials recognized that "verification" of a ban with the Soviets "would be extremely difficult" because so many space systems deployed for other purposes could also be used as weapons.[66] During negotiations, the Soviets made "frequent" requests to include the forthcoming US Space Shuttle, a civilian capability from the American point of view, on the list of banned ASAT systems.[67] The Americans refused to limit the shuttle since it would "not be used as an ASAT system in any respect," but struggled to devise provisions for the Soviets to verify this claim.[68] The United States in turn had concerns about the Soviets hiding ASAT capabilities on satellites.[69] These disagreements about how to distinguish between peaceful platforms and orbital weapons stalled diplomacy well before the Soviet invasion of Afghanistan ended détente in December 1979. Despite signing the SALT II agreement in June 1979 over distinguishable ballistic

60. Bahney, Pearl, and Markey 2019.
61. Acton 2018.
62. CIA, "Outlook for Rapid Expansion."
63. Presidential Directive/NSC-54, "Civil Operational Remote Sensing," 16 November 1979. NSA.
64. Early 2014.
65. Presidential Directive/NSC–37, 11 May 1978. FRUS, 1977–80, vol. XXVI, Arms Control and Nonproliferation, doc. 27.
66. Summary of Significant Discussion and Conclusions of a Policy Review Committee Meeting, 4 August, 1977. FRUS, 1977–80, vol. XXVI, Arms Control and Nonproliferation, doc. 5.
67. Telegram from the Embassy in Finland to the Department of State, 20 June 1978. FRUS, 1977–80, vol. XXVI, Arms Control and Nonproliferation, doc. 33.
68. Memorandum from Aaron to Brzezinski, 30 May 1979. FRUS, 1977–80, vol. XXVI, Arms Control and Nonproliferation, doc. 52.
69. Telegram from the Embassy in Austria to the Department of State, 13 June 1979. FRUS, 1977–80, vol. XXVI, Arms Control and Nonproliferation, doc 54.

missile systems, the superpowers made little progress in negotiating limits over indistinguishable space systems.

In the early 1980s, the Soviet Union approached the United States with fresh proposals for limiting ASAT weapons in space.[70] Secretary of State George Shultz rejected these efforts "because of verification problems" associated with the distinction between civil and military space capabilities.[71] In a 1984 report to Congress, the Reagan administration made explicit how the duality of space systems created twin detection and disclosure barriers to cooperation. "The fact that ASAT capabilities are inherent in some systems developed for other missions," the report argued, "makes it impossible to verify compliance" with a comprehensive ban.[72] Cooperative monitoring measures would be needed to determine whether satellites or spacecraft masked ASAT capabilities. While recognizing that distinguishability could in principle be overcome with inspections, the report underscored the severe costs involved due to the highly integrated nature of space technology, stating that "disclosure of information" from such inspections could "create an unacceptable risk," not only to US military capabilities but also to civilian uses of space (Figure 1).

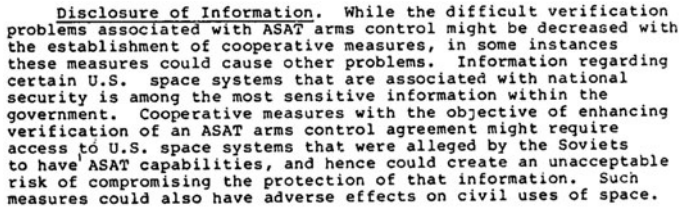
Disclosure of Information. While the difficult verification problems associated with ASAT arms control might be decreased with the establishment of cooperative measures, in some instances these measures could cause other problems. Information regarding certain U.S. space systems that are associated with national security is among the most sensitive information within the government. Cooperative measures with the objective of enhancing verification of an ASAT arms control agreement might require access to U.S. space systems that were alleged by the Soviets to have ASAT capabilities, and hence could create an unacceptable risk of compromising the protection of that information. Such measures could also have adverse effects on civil uses of space.

FIGURE 1. *Excerpt from the Reagan administration report on anti-satellite arms control (Presidential Report to Congress, "US Policy on ASAT Arms Control," 31 March 1984, p. 5)*

This tension between detection and disclosure also haunted the prospects for cooperation as a new round of ASAT talks began in the late 1980s. To verify any ASAT ban, US officials stressed "the importance of on-site inspection and international observer teams," but were unwilling to accept the security risks associated with these

70. Stares 1987, 148.

71. Memorandum from Shultz to Reagan, "Meeting with Dobrynin," 6 April 1984. FRUS, 1981–88, vol. IV, 1983–85 Soviet Union, doc. 209.

72. Presidential Report to Congress, "US Policy on ASAT Arms Control."

cooperative measures.[73] The superpowers ultimately failed to resolve the verification issue for ASAT, even as both sides devised a complex inspection regime to verify missile limits under the 1987 INF Treaty and the 1991 START Treaty.

The failed arms negotiations over ASAT weapons lend strong support for our theory. Consistent with our expectations for H2, the superpowers confronted severe information problems once space technology became indistinguishable and ubiquitous during the 1970s. In sharp contrast to the earlier era of easy detection, verifying the peaceful uses of orbital platforms became impractical without inspections. But the Americans worried that letting the Soviets observe integrated space systems could disclose "the most sensitive information" about US military forces and economic capabilities (Figure 1). Multiple efforts to manage the arms race in space therefore failed.

H3: Technology creates a severe but surmountable detection constraint

To assess H3 we examine indistinguishable but niche technologies. Six cases exhibit these variables: (1) biotechnology before the molecular biology revolution (1915–1953); (2) early firearm technology (1520–1840); (3) long-range rockets before the maturation of missile platforms (1944–1970); (4) chemical technology, because the weapons occupied a niche role in military enterprises (1850–2020); (5) hypersonic vehicles (1981–2020); and (6) nuclear technology (1945–2020), specifically the capacity to produce the fissile material that fuels the explosive core of atomic weapons.

Arms control agreements failed to emerge over early rockets, pre-nineteenth-century firearms, and hypersonic vehicles. The dual use detection problem with rocket technology in the early 1960s aligns with H3: sometimes states will not be able to devise monitoring solutions to differentiate military from civilian applications. The pre-nineteenth-century firearm and recent hypersonic cases offer neutral support—neither supporting nor contradicting our hypothesis—as other factors made arms control unattractive in both cases, and the separate effect of technology attributes is difficult to isolate. Stronger support comes from the type of agreements that emerged over early biological, chemical, and nuclear technology. In these cases, we find explicit recognition from governments that the indistinguishable nature of technology created detection problems. But states were able to surmount this constraint by narrowing the scope of agreements and/or devising monitoring measures. For example, the 1925 Geneva Protocol curtailed only the most observable battlefield use of chemical and biological weapons. In the appendix, we also assess the negotiations around the 1993 Chemical Weapons Convention because the technology exhibited a unique mix of low military integration and high commercial integration, which led industrial actors to press for limits on an inspection regime that would protect their trade secrets.

73. Memorandum from McFarlane to Reagan, "Geneva Arms Control Talks," 7–8 January 1985. FRUS, 1981–88, vol. IV, 1983–85 Soviet Union, doc. 346. But see Bateman 2022.

The nuclear case allows us to evaluate the explanatory power of our variables relative to existing explanations. Some scholars argue that the most powerful states in the international system had strong mutual incentives to inhibit the spread of nuclear weapons in the 1960s.[74] As a result, the superpowers colluded to establish the 1968 Nuclear Nonproliferation Treaty (NPT) and even coerced non-nuclear-weapon states into joining this multilateral institution.[75] Others show that savvy non-nuclear-weapon states wrested concessions from Washington or Moscow in exchange for NPT accession.[76] Yet these accounts miss how the dual use nature of nuclear technology enabled such arms control bargains to be struck.[77] The difficulty of distinguishing military from peaceful endeavors in the nuclear realm saddled the NPT with detection problems.[78] However, states were willing to allow intrusive inspections of nuclear facilities precisely because this niche technology created manageable security risks from information disclosure.

Nuclear technology exemplified all four indistinguishability attributes. First, nuclear weapons relied on production facilities with physical characteristics identical to atomic energy enterprises. The same plant for enriching fuel in civilian power plants or reprocessing radioactive waste could produce fissile material—enriched uranium or plutonium—for the explosive core of a bomb. As a senior US official lamented in 1955, many countries with atomic energy ambitions could produce "large quantities of fissionable material equally useful for peaceful or military purposes. This is not a pleasant prospect."[79] Second, the development pathway for pursuing the bomb overlapped with peaceful activities until the final weaponization stage. "Once a nation has a civilian atomic energy program encompassing fairly large reactors and processing facilities," a CIA report underscored in 1957, "it requires only relatively little investment … to initiate a weapons program."[80] Third, weapons programs could emulate peaceful fissile material production plants. As a 1963 NIE on proliferation highlighted, "The plutonium route to a weapons program has become a well-marked trail, and one which in its earlier stages is scarcely distinguishable from a purely peaceful program."[81] Finally, the conversion speed rapidly increased as a state accumulated fissile material. This meant that "the nations with the most developed peaceful programs will be nearest to a military bomb capability," the State Department concluded in 1968.[82]

74. Brands 2007; Gavin 2012.
75. Coe and Vaynman 2015; Gibbons 2022; Miller 2018.
76. Schrafstetter and Twigge 2004; Volpe 2023.
77. But see Pauly 2022.
78. Fuhrmann 2012.
79. Gerard C. Smith, "Observations on the Problem of Controlling Against Diversion of Fissionable Material from Nuclear Power," Department of State, 17 September 1955. NSA no. NN00050.
80. NIE, "Nuclear Weapons Production in Fourth Countries: Likelihood and Consequences," Director of Central Intelligence, 18 June 1957. NSA.
81. NIE, "Likelihood and Consequences of a Proliferation of Nuclear Weapons Systems," Director of Central Intelligence, 28 June 1963. NSA.
82. Henry Owen to Dean Rusk, "After NPT, What," Department of State, 10 June 1968. NSA.

Nuclear technology also exhibits low integration because the range and variety of uses have long been limited to select applications. Within military enterprises, nuclear weapons perform a narrow subset of missions focused on strategic deterrence, albeit with significant consequences. Within the civilian economy, nuclear technology primarily occupies a niche role in energy generation, though again with potentially major returns in electricity production. In both realms, nuclear assets are rather isolated from other activities or infrastructure systems, often for physical safety and security reasons. In addition, the cost of developing atomic weapons or energy enterprises is high.

The indistinguishable nature of nuclear technology drove up the detection needs for verifying peaceful uses. In 1955, US officials anticipated that on-site inspections of civil nuclear programs, with "complete access to plants and full operational knowledge," would be necessary to check compliance with early nonproliferation obligations.[83] British experts also concluded that the "diversion [of] nuclear fuel from such [civil] power stations [for] military purposes could be prevented only by [an] effective system [of] inspection and accounting."[84]

In 1968, the NPT set the multilateral foundation to prohibit the acquisition of nuclear weapons. The agreement narrowly focused on banning weapons. Production of fissile material was left open as a permitted activity, so long as states allowed the International Atomic Energy Agency (IAEA) to verify peaceful uses. "The treaty would be ineffective in many countries without safeguards," a senior US official argued in 1967, because "the location of nuclear facilities can often be ascertained by unilateral means, but what goes on in those facilities is usually impossible to determine without inspection."[85] Verifying compliance with the NPT would therefore require an intrusive monitoring regime.

The niche nature of nuclear technology helps explain why states accepted such intensive inspections: they faced modest security risks from information disclosure. IAEA inspections of an atomic energy program would provide little insight into a state's capacity to field force beyond the nuclear realm. Even total access to civilian nuclear facilities was unlikely to illuminate broader metrics of military power, such as the disposition of conventional weapons or military facilities. Instead, inspections promised to reveal information about nuclear latency—the narrow capacity to build atomic weapons that lingered within all peaceful nuclear enterprises.[86] This technical data could improve an adversary's ability to target nuclear facilities in a future conflict, but would be less relevant to war plans against nonnuclear capabilities.

Yet many states also saw disclosure of civilian programs as beneficial in helping to alleviate adversarial concerns about nuclear latency. The archival record of private

83. Smith, "Observations on the Problem."
84. Franklin C. Gowen, "Nuclear Safeguards Discussions," Department of State, 5 August 1955. NSA no. NN00029.
85. Philip J. Farley, "Safeguards Provision of NPT," Department of State, 5 December 1967. NSA no. NN02095.
86. Mehta and Whitlark 2017.

discussions between the United States and West Germany illustrates this dynamic. Bonn played a key role in negotiating the verification protocols for the NPT.[87] In 1967, West German officials worried that the Soviets would send IAEA inspectors "to carry out industrial espionage in the Western non-nuclear countries in regard to nuclear technology."[88] But Bonn made no mention of security risks beyond the civil nuclear program. Instead, German officials recognized that such inspections enabled Moscow to verify that Bonn was not building the bomb in secret, which decreased incentives to attack Germany.[89] Given the isolation of nuclear technology, the West German experience illustrates how states can let adversaries inspect their atomic weapons potential without revealing vulnerabilities in broader aspects of military power.

H4: Technology creates a severe but manageable disclosure constraint

To evaluate this final hypothesis, we examine arms control outcomes over distinguishable technologies with high integration. Many conventional military capabilities with civilian counterparts exhibit these dual use characteristics—sixteen technologies fall in this zone. We find that states achieved agreements to limit the military uses to some degree in many cases. Airships, railcars, and torpedoes offer neutral support because the role of technology is difficult to isolate in these cases where postwar armament controls were imposed on defeated nations. But an examination of verification measures across the other cases lends strong support for H4 by revealing how states took two specific steps to manage the risks from information disclosure.

First, to avoid disclosures from inspection, states often relied on their intelligence collection capabilities to verify compliance. In eight instances, agreements to limit military uses emerged without any cooperative monitoring measures. Restrictions on strategic air defense, conventional explosives, early drones, modern firearms, laser weapons, machine guns, maritime vessels, and nonstrategic submarines all used unilateral information gathering or "national technical means" of verification. Avoiding on-site inspections effectively sidestepped the disclosure problem associated with these highly integrated technologies.

The option of unilateral monitoring was available only because the military capabilities could be easily distinguished from their peaceful cousins. The Washington (1922) and London (1930) Naval Treaties illustrate this mechanism at work. These agreements established tonnage limits on capital ships (battleships) and aircraft carriers for each great naval power as well as design and size limits on destroyers, submarines, and auxiliary ships. Yet they lacked cooperative monitoring provisions.[90] Military ships had observable features their civilian counterparts lacked: large-

87. Schrafstetter and Twigge 2004.

88. Thomas L. Hughes to the Secretary, "Reasons for West German Opposition to the Non-Proliferation Treaty," Department of State, 1 March 1967. Wilson Center Digital Archive.

89. Volpe 2023, 105, 109–111.

90. Burns 1968.

caliber guns, heavy armor, and advanced propulsion systems. The construction of warships often followed a bespoke process, whereas commercial ships were mass-produced with simpler steel forming and welding processes. These attributes made it easier for intelligence services to determine the civil or military nature of construction at shipyards, and verify whether military vessels met the treaty limitations.[91]

Second, when greater monitoring measures were needed, states devised restrictive verification protocols for on-site inspections based on geography or physical access. In seven instances, the need for more transparency was due to reasons beyond the dual use nature of the technology. Tactical air defense, aircraft, armored vehicles, artillery, cruise missiles, and strategic submarines were all highly distinguishable. But the mobility and/or small size of these weapon platforms often drove the need for inspections in the Korean Armistice Agreement, as well as the Peace Treaty between Israel and Egypt, to verify caps on specific conventional weapons. However, national inspection teams could verify numbers only at designated ports of entry (Korean Armistice) or in certain territorial zones (Israel and Egypt). Later in the Cold War, states had to devise transparency measures that would demonstrate compliance with numerical limits on smaller (easier to hide) combat aircraft and armored vehicles without revealing information about broader military capabilities. The 1990 Treaty on Conventional Armed Forces in Europe included on-site inspections to verify conventional armament limitations among the signatories. But it also put temporal and geographic limits on inspections to dampen the security risks from information disclosure.

States also phased out inspections to limit disclosure damage. The 1987 INF treaty between the United States and the Soviet Union banned all ground-launched ballistic and cruise missiles with intermediate ranges (500 to 5,500 km). In contrast to their ICBM brethren, shorter-range rockets and cruise missiles were highly integrated within military enterprises because they could perform a wider variety of missions at lower cost. This technology feature led American and Soviet officials to worry that inspections would be used to observe other weapons capabilities and plants.[92] The treaty called for the elimination of these missiles, which was verified with highly intrusive inspections, but after a set period, inspections would end, and states would rely on their intelligence capabilities to verify compliance. Phasing out inspections helped dampen the security risks associated with long-term observation of military units and installations.

The types of arms control agreements that emerged over distinguishable technologies with ubiquitous military application align with our expectations for H4. Some scholars claim that the offensive and expensive nature of some conventional strike capabilities made them prime candidates for arms control.[93] Yet our results indicate that states often circumscribed cooperation—relying on unilateral intelligence

91. Goldman 1994, 178–80.
92. Glitman 2006, 210–11.
93. Glaser 2010, 228–56; Jervis 1978.

collection or restricted inspections—to manage the security risks associated with high military integration.

Conclusion

Dual use technologies often present extra challenges for efforts to limit military competition. Our study reveals why this is the case. The duality of technology alters the information needed to detect compliance without disclosing deeper military and commercial secrets. As key dimensions—distinguishability between military and civilian applications and integration with other activities—vary, so do prospects for cooperation.

Many past academic treatments of technology in international relations lacked the conceptual clarity and standardization to make technological attributes a useful variable for developing and testing midlevel theories. Technology has been more of a general topic area for research rather than an independent variable to explain phenomena. This article engages in concept formation by identifying cross-cutting technology attributes, theorizing their effects, and developing measurement criteria to empirically bin the universe of capabilities into distinct categories.[94]

The substantive contribution of this article is to reveal how dual use technology attributes constrain the options for creating cooperative institutions. The detection and disclosure problems intersect with other factors that shape arms control outcomes. The balance of power, for example, undoubtedly affects whether and how states form agreements. But future research should assess whether these variables are conditional on the technologies involved. Power balances or domestic politics could play a strong role when the technology poses few constraints but become quite muted when dual use concerns present the most significant obstacles to cooperation. For instance, many argue that parity is essential for states to consider arms control limitations. They may well be right—China today seems unwilling to contemplate arms control until it catches up with the United States. But our framework suggests that there will be considerable variation in cooperation outcomes even under this condition. If Beijing reaches parity by building up nuclear-tipped ICBMs, this type of technology should dampen the dual use issue as a constraint on arms control. By contrast, an arms race over technologies in the dead zone, such as cyber weapons or space platforms, could undermine the prospects for cooperation, even if both sides see benefits from mutual restraint.

Looking ahead to contemporary emerging technologies, our results not only imply that policy efforts to control artificial intelligence (AI) will face insurmountable challenges, but also illuminate why that is the case. AI refers to computing capabilities that use algorithms to learn from data and make decisions without human intervention. The consensus view is that this technology will reshape the foundations of

94. Adcock and Collier 2001.

military and economic power.[95] Managing AI with international institutions is also assumed to be impossible. This forecast is highly intuitive but poorly understood—what is it about AI that would make international governance particularly difficult? Uncertainty about the effects of concrete applications may be a factor in the short term. But our theory suggests that the tension between detection and disclosure will doom the prospects for cooperation even as that uncertainty decreases. Military AI systems will likely be indistinguishable from their peaceful counterparts, with any discernible indicators of end use buried within the opaque source code for each respective system. Even if distinct military uses for AI emerge in the future, distinguishing these military systems from their civilian cousins will require high detection levels, such as access to the inner workings of AI systems. However, AI is also poised to become highly integrated within military and civilian realms as an enabling technology for numerous other capabilities. States are therefore likely to balk at disclosures of AI algorithms for fear that even seemingly limited information could allow insights into other sensitive military forces or commercial products. The effects of these technology factors will obstruct prospects for international controls on military AI applications beyond the challenges from uncertainty, lack of parity, or disagreement about mutual interest.

The information problems we identify do suggest a possible alternative to managing emerging technologies in the years ahead. When technologies such as AI fall in the dead zone for arms control, states may have a more promising path forward if they focus more on managing behaviors than on limiting capabilities. This implies a need to observe the effects of actions rather than the development or possession of technology. The downside to this approach is that states can respond to a violation only after the damage is done. But this risk may be tolerable because it sidesteps some of the severe detection and disclosure problems rooted in many emerging technologies today. Governance efforts to develop international institutions should consider this alternative when the dual use nature of technology renders traditional arms control agreements unverifiable.

Supplementary Material

Supplementary material for this article is available at <https://doi.org/10.1017/S0020818323000140>.

References

Abbott, Kenneth W. 1993. Trust but Verify: The Production of Information in Arms Control Treaties and Other International Agreements. *Cornell International Law Journal* 26 (1):1–58.

95. Favaro, Renic, and Kühn 2022; Horowitz 2020.

Acton, James M. 2018. Escalation Through Entanglement: How the Vulnerability of Command-and-Control Systems Raises the Risks of an Inadvertent Nuclear War. *International Security* 43 (1):56–99.
Adcock, Robert, and David Collier. 2001. Measurement Validity: A Shared Standard for Qualitative and Quantitative Research. *American Political Science Review* 95 (3):529–46.
Bahney, Benjamin W., Jonathan Pearl, and Michael Markey. 2019. Antisatellite Weapons and the Growing Instability of Deterrence. In *Cross-Domain Deterrence: Strategy in an Era of Complexity*, edited by Jon R. Lindsay and Erik Gartzke, 121–43. Oxford University Press.
Bateman, Aaron. 2022. Mutually Assured Surveillance at Risk: Anti-Satellite Weapons and Cold War Arms Control. *Journal of Strategic Studies* 45 (1):119–42.
Brands, Hal. 2007. Non-proliferation and the Dynamics of the Middle Cold War: The Superpowers, the MLF, and the NPT. *Cold War History* 7 (3):389–423.
Bresnahan, Timothy F., and M. Trajtenberg. 1995. General Purpose Technologies "Engines of Growth?" *Journal of Econometrics* (25):83–108.
Bunn, George. 1992. *Arms Control by Committee: Managing Negotiations with the Russians*. Stanford University Press.
Burns, Richard Dean. 1968. Inspection of the Mandates, 1919–1941. *Pacific Historical Review* 37 (4):445–62.
Burrows, William E. 1999. *This New Ocean: The Story of the First Space Age*. Modern Library.
Carnegie, Allison, and Austin Carson. 2020. *Secrets in Global Governance: Disclosure Dilemmas and the Challenge of International Cooperation*. Cambridge University Press.
Chyba, Christopher F. 2020. New Technologies and Strategic Stability. *Daedalus* 149 (2):150–70.
Coe, Andrew J., and Jane Vaynman. 2015. Collusion and the Nuclear Nonproliferation Regime. *Journal of Politics* 77 (4):983–97.
Coe, Andrew J., and Jane Vaynman. 2020. Why Arms Control Is So Rare. *American Political Science Review* 114 (2):342–55.
Cowan, Robin, and Dominique Foray. 1995. Quandaries in the Economics of Dual Technologies and Spillovers from Military to Civilian Research and Development. *Research Policy* 24 (6):851–68.
Debs, Alexandre, and Nuno P. Monteiro. 2014. Known Unknowns: Power Shifts, Uncertainty, and War. *International Organization* 68 (1):1–31.
Ding, Jeffrey, and Allan Dafoe. 2023. Engines of Power: Electricity, AI, and General-Purpose, Military Transformations. *European Journal of International Security* 8 (3):377–94.
Early, Bryan R. 2014. Exploring the Final Frontier: An Empirical Analysis of Global Civil Space Proliferation. *International Studies Quarterly* 58 (1):55–67.
Favaro, Marina, Neil Renic, and Ulrich Kühn. 2022. "Negative Multiplicity: Forecasting the Future Impact of Emerging Technologies on International Stability and Human Security." Institute for Peace Research and Security Policy, University of Hamburg.
Fuhrmann, Matthew. 2012. *Atomic Assistance: How "Atoms for Peace" Programs Cause Nuclear Insecurity*. Cornell University Press.
Gartzke, Erik, and Jon R. Lindsay. 2015. Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace. *Security Studies* 24 (2):316–48.
Gavin, Francis J. 2012. *Nuclear Statecraft: History and Strategy in America's Atomic Age*. Cornell University Press.
Gibbons, Rebecca Davis. 2022. *The Hegemon's Tool Kit: US Leadership and the Politics of the Nuclear Nonproliferation Regime*. Cornell University Press.
Gilli, Andrea, and Mauro Gilli. 2019. Why China Has Not Caught Up Yet: Military-Technological Superiority and the Limits of Imitation, Reverse Engineering, and Cyber Espionage. *International Security* 43 (3):141–89.
Glaser, Charles L. 2000. The Cause and Consequences of Arms Races. *Annual Review of Political Science* 3 (1):251–76.
Glaser, Charles L. 2010. *Rational Theory of International Politics: The Logic of Competition and Cooperation*. Princeton University Press.
Glitman, Maynard W. 2006. *The Last Battle of the Cold War: An Inside Account of Negotiating the Intermediate Range Nuclear Forces Treaty*. Palgrave Macmillan.

Goertz, Gary. 2017. *Multimethod Research, Causal Mechanisms, and Case Studies: An Integrated Approach*. Princeton University Press.
Goldman, Emily O. 1994. *Sunken Treaties: Naval Arms Control Between the Wars*. Pennsylvania State University Press.
Green, Brendan Rittenhouse. 2020. *The Revolution that Failed: Nuclear Competition, Arms Control, and the Cold War*. Cambridge University Press.
Green, Brendan Rittenhouse, and Austin Long. 2020. Conceal or Reveal? Managing Clandestine Military Capabilities in Peacetime Competition. *International Security* 44 (3):48–83.
Hendrickx, Bart, and Dwayne A. Day. 2020. Target Moscow: Soviet Suspicions About the Military Uses of the American Space Shuttle. *Space Review*, 27 January. Available at <https://www.thespacereview.com/article/3873/1>.
Horowitz, Michael C. 2010. *The Diffusion of Military Power: Causes and Consequences for International Politics*. Princeton University Press.
Horowitz, Michael C. 2020. Do Emerging Military Technologies Matter for International Politics? *Annual Review of Political Science* 23 (1):385–400.
Jervis, Robert. 1978. Cooperation Under the Security Dilemma. *World Politics* 30 (2):167–214.
Jovanovic, Boyan, and Peter L. Rousseau. 2005. *General Purpose Technologies*. National Bureau of Economic Research. Available at <http://www.nber.org/papers/w11093>.
Kalic, Sean N. 2012. *US Presidents and the Militarization of Space, 1946–1967*. Texas A&M University Press.
Kardon, Isaac B., and Wendy Leutert. 2022. Pier Competitor: China's Power Position in Global Ports. *International Security* 46 (4):9–47.
Koblentz, Gregory D. 2009. *Living Weapons: Biological Warfare and International Security*. Cornell University Press.
Koremenos, Barbara. 2001. Loosening the Ties that Bind: A Learning Model of Agreement Flexibility. *International Organization* 55 (2):289–325.
Kreps, Sarah E. 2018. The Institutional Design of Arms Control Agreements. *Foreign Policy Analysis* 14 (1):127–47.
Kucik, Jeffrey, and Eric Reinhardt. 2008. Does Flexibility Promote Cooperation? An Application to the Global Trade Regime. *International Organization* 62 (3):477–505.
Kydd, Andrew. 2000. Arms Races and Arms Control: Modeling the Hawk Perspective. *American Journal of Political Science* 44 (2):228–44.
Lieber, Keir A. 2008. *War and the Engineers: The Primacy of Politics over Technology*. Cornell University Press.
Lieber, Keir A., and Daryl G. Press. 2017. The New Era of Counterforce: Technological Change and the Future of Nuclear Deterrence. *International Security* 41 (4):9–49.
Lindsey, David. 2015. Military Strategy, Private Information, and War. *International Studies Quarterly* 59 (4):629–40.
Lin-Greenberg, Erik, and Theo Milonopoulos. 2021. Private Eyes in the Sky: Emerging Technology and the Political Consequences of Eroding Government Secrecy. *Journal of Conflict Resolution* 65 (6):1067–97.
Lipsey, Richard G., Kenneth I. Carlaw, and Clifford T. Bekar. 2005. *Economic Transformations: General Purpose Technologies and Long-Term Economic Growth*. Oxford University Press.
Mantilla, Giovanni. 2023. Deflective Cooperation: Social Pressure and Forum Management in Cold War Conventional Arms Control. *International Organization* 77 (3):564–98.
Matovski, Aleksandar. 2020. Strategic Intelligence and International Crisis Behavior. *Security Studies* 29 (5):964–90.
Maurer, John D. 2022. *Competitive Arms Control: Nixon, Kissinger, and SALT, 1969–1972*. Yale University Press.
Mehta, Rupal N., and Rachel Elizabeth Whitlark. 2017. The Benefits and Burdens of Nuclear Latency. *International Studies Quarterly* 61 (3):517–28.
Miller, Nicholas L. 2018. *Stopping the Bomb: The Sources and Effectiveness of US Nonproliferation Policy*. Cornell University Press.

Moltz, James Clay. 2008. *The Politics of Space Security: Strategic Restraint and the Pursuit of National Interests*. Stanford University Press.
Paine, Taunton. 2018. Bombs in Orbit? Verification and Violation Under the Outer Space Treaty. *Space Review*, 19 March. Available at <https://www.thespacereview.com/article/3454/1>.
Pauly, Reid B. C. 2022. Deniability in the Nuclear Nonproliferation Regime: The Upside of the Dual-Use Dilemma. *International Studies Quarterly* 66 (1):1–13.
Reppy, Judith. 2006. Managing Dual-Use Technology in an Age of Uncertainty. *The Forum* 4 (1).
Richelson, Jeffrey T. 2015. US Intelligence and the Soviet Space Program. National Security Archive Electronic Briefing Book no. 501. Available at <https://nsarchive2.gwu.edu//NSAEBB/NSAEBB501/>.
Rovner, Joshua. 2020. What Is an Intelligence Contest? *Texas National Security Review* 3 (4):115–20.
Schelling, Thomas C., and Morton H. Halperin. 1961. *Strategy and Arms Control*. Potomac Books.
Schneider, Jacquelyn. 2019. The Capability/Vulnerability Paradox and Military Revolutions: Implications for Computing, Cyber, and the Onset of War. *Journal of Strategic Studies* 42 (6):841–63.
Schrafstetter, Susanna, and Stephen Twigge. 2004. *Avoiding Armageddon: Europe, the United States, and the Struggle for Nuclear Non-proliferation, 1945–1970*. Praeger.
Sechser, Todd S., Neil Narang, and Caitlin Talmadge. 2019. Emerging Technologies and Strategic Stability in Peacetime, Crisis, and War. *Journal of Strategic Studies* 42 (6):727–35.
Stares, Paul. 1987. *Space and National Security*. Brookings Institution Press.
Talmadge, Caitlin. 2019. Emerging Technology and Intra-war Escalation Risks: Evidence from the Cold War, Implications for Today. *Journal of Strategic Studies* 42 (6):864–87.
Volpe, Tristan A. 2019. Dual-Use Distinguishability: How 3D-Printing Shapes the Security Dilemma for Nuclear Programs. *Journal of Strategic Studies* 42 (6):814–40.
Volpe, Tristan A. 2023. *Leveraging Latency: How the Weak Compel the Strong with Nuclear Technology*. Oxford University Press.
Williams, Heather. 2019. Asymmetric Arms Control and Strategic Stability: Scenarios for Limiting Hypersonic Glide Vehicles. *Journal of Strategic Studies* 42 (6):789–813.
Zegart, Amy B. 2022. *Spies, Lies, and Algorithms: The History and Future of American Intelligence*. Princeton University Press.

Authors

Jane Vaynman is Assistant Professor in the Department of Political Science at Temple University, Philadelphia, Pennsylvania. She can be reached at jane.vaynman@temple.edu.
Tristan A. Volpe is Assistant Professor in the Defense Analysis Department at the Naval Postgraduate School, Monterey, California and Nonresident Fellow in the Nuclear Policy Program at the Carnegie Endowment for International Peace, Washington, DC. He can be reached at tvolpe1@nps.edu.

Acknowledgments

Authors listed in alphabetical order. For excellent feedback on prior drafts, we thank John Arquilla, Austin Carson, Fiona Cunningham, Jennifer Erickson, Michael Freeman, Matt Fuhrmann, Charles Glaser, Amoz Hor, Michael Horowitz, Greg Koblentz, Ulrich Kühn, Keir Lieber, Nicholas Miller, Aidan Milliff, Reid Pauly, Josh Rovner, Jacquelyn Schneider, Todd Sechser, Robert Trager, Camber Warren, and Heather Williams; and seminar participants at the 2023 Yale Nuclear Security Symposium, the CSIS-IFSH Arms Control and Emerging Tech Working Group, UCLA's International Relations Workshop, George Washington University's Institute for Security and Policy Studies, University of Pennsylvania's Perry World House, Carnegie's Nuclear Policy Program, and the *IO* editors and reviewers. For superb research assistance, we are indebted to Dominic Cruz Bustillos, Mat Couillard, Gregory Hillman, Cyrus Jabbari, Zak Kallenborn, Jordan Miller, Michael Noonan, Eric Perinovic, Ian Rice, Cavender Sutton, Jamie Withorne,

and especially Brian Rose. The views in this article are the authors' own and do not reflect those of the Department of Defense, the Department of State, or the US government.

Funding

This work was supported by the John D. and Catherine T. MacArthur Foundation [G-1802-152803] and the CWMD Systems Office in the Office of the Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs.

Key Words

Technology; international cooperation; arms control; dual use; international institutions; international security; bargaining; information; military technology; competition; secrecy

Date received: May 19, 2022; Date accepted: June 26, 2023