The Scholar

Texas National Security Review: Volume 4, Issue 4 (Fall 2021)
Print: ISSN 2576-1021 Online: ISSN 2576-1153

BETTER MONITORING AND BETTER SPYING: THE IMPLICATIONS OF EMERGING TECHNOLOGY FOR ARMS CONTROL

Jane Vaynman

How will emerging technology affect prospects for arms control? Technologies such as small satellites and artificial intelligence (AI) have applications in arms control monitoring and can affect the amount of information collected or the ease of information processing. While intuition suggests that technologies that improve monitoring should make arms control easier to achieve, this is not always the case. In considering agreements, states face a trade-off between beneficial and adverse aspects of information. States need transparency to observe behavior and assure compliance, but the same information used to monitor an agreement can also be used to gain a military advantage. Monitoring that allows for more effective espionage will mean that transparency comes at the expense of high threats to security. Three key factors are important in assessing the potential impact of any technology: how it affects unilateral monitoring capabilities; the degree to which it allows demonstrable control over information; and the effect that it has on concealment. These factors provide a framework to analyze the likely effects of emerging technologies, four of which are addressed here: small satellites, drones, AI, and digital additive manufacturing.

Introduction

How will emerging technology affect whether states are able to use arms control as a foreign policy tool to manage competition? Will advances in artificial intelligence (AI), for example, make it any easier for states to agree to limit conventional weapons, nuclear capabilities, or risky behaviors? Much attention has previously been paid to the role that international cooperation might play in controlling the spread of emerging technologies themselves. But irrespective of the prospects for such efforts, emerging technology is likely to also play an important role in arms control by affecting the capability of states to monitor and verify compliance. Analysts have already started to think about how technology can improve monitoring,[1] leading to intuitions that having greater access to information about compliance will make states more likely to sign agreements. However, more information is not always better, and under some conditions, more effective monitoring may actually undermine cooperation efforts. In assessing the effects of emerging technology on arms control, it is important to consider the countervailing impacts of information collection on state security interests.

Arms control agreements allow states to avoid the costs of an arms race or, more generally, of a status quo in which both sides expend resources

[1] Alexander Graef and Moritz Kutt, "New Opportunities to Build Trust and Ensure Compliance: Using Emerging Technologies for Arms Control and Verification," in *Capturing Technology, Rethinking Arms Control: Conference Reader* (Berlin: Institute for Peace Research; Security Policy at the University of Hamburg, 2020), 27–34, https://rethinkingarmscontrol.de/wp-content/uploads/2020/10/20-AA-RAC-Reader-2020-10-28-final-korr-kompr.pdf; National Academies of Sciences, Engineering, and Medicine, *Nuclear Proliferation and Arms Control Monitoring, Detection, and Verification: A National Security Priority: Interim Report* (Washington, DC: National Academies Press, 2021), 100, https://doi.org/10.17226/26088; and Ankit Panda, et al., eds. *New Approaches to Verifying and Monitoring North Korea's Nuclear Arsenal*, Carnegie Endowment for International Peace, 2021. For a policymaker perspective on opportunities of emerging technology for arms control verification, see "Remarks by Rose Gottemoeller, Acting Under Secretary for Arms Control and International Security," Moscow State Institute of International Relations (MGIMO) Moscow, Russia, March 30, 2012, https://geneva.usmission.gov/2012/04/02/rose-gottemoeller-arms-control-in-the-information-age/.

or take on risks in an effort to gain a security advantage over the other.[2] As such, agreements can be beneficial even for competing states, especially in cases where arms racing essentially maintains the status quo. The most well-known "cost" of arms control — and the reason that is usually presented for why states fail to sign agreements — is the risk of cheating.[3] States can face severe security threats if an adversary secretly violates a deal and gains a military advantage. In theory, the risk of cheating could be addressed through monitoring. If one side can see everything the other is doing, there is no way to gain a temporary advantage. Violations would immediately be detected and the other side could respond with its own arms buildup. The solution for getting countries to sign more agreements, it would seem, would be to increase monitoring and transparency in order to decrease the fear of cheating. However, this approach misses an often-unappreciated side effect: increased risks to a state's security that are created through the effective implementation of a deal.

States collect information to verify agreement compliance, but the same information can also aid intelligence and espionage. The behaviors involved in observing agreement-mandated limits or restrictions — such as inspectors visiting a site where capabilities are being manufactured or destroyed — could allow the observing state to collect information about potential military vulnerabilities of its opponent.[4] The collection of this additional information may be intentional, in the form of military espionage. Or, the information needed to verify the agreement may serve a dual purpose, making the collection of the additional information unavoidable. For example, to verify that a weapon is not deployed at military bases, states would have to reveal the locations of those bases, making them possible targets in a future military conflict. While the actors involved in arms control monitoring, such as government agencies or international organizations, tend to dislike their activities being referred to as intelligence collection, both practitioners and scholars recognize, at least in part, the connection between monitoring and intelligence gathering.[5] To varying degrees, where monitoring compliance also reveals vulnerabilities, there is a trade-off between transparency and security, where the costs to security may well outweigh the benefits that result from a deal.[6]

A transparency-security trade-off is a feature of any agreement with monitoring and verification provisions. The severity of this trade-off — i.e., the degree to which transparency creates security costs — depends on a number of factors.[7] For example, these factors include whether different types of capabilities are co-located and the extent of existing openness into a state's security establishment. Another particularly important factor is the tools that are available for collecting compliance information. If compliance is verified by, for example, human eyes looking at a battleship, the state being inspected would be concerned about what else that person might see at a naval base while arriving, leaving, or even while collecting dust on their shoes.[8] Changes in the way that monitoring is conducted, caused by innovation in the technology of information collection and information processing, are likely to affect the transparency-security trade-off, and in doing so, have an impact on when states come to an agreement.

This article expands on the concept of the transparency-security trade-off in arms control agreements by considering how the trade-off may change if emerging technologies such as AI and advanced satellites start to play a bigger role in security cooperation. Although there has been increasing scholarly focus on the effects of emerging technologies on other outcomes of interest in international security, such as the nature of conflict,[9] strategic

[2] Andrew Kydd, "Arms Races and Arms Control: Modeling the Hawk Perspective," *American Journal of Political Science* 44, no. 2 (April 2000): 228–44, https://www.jstor.org/stable/2669307

[3] Steven E. Miller, "Arms Control in a World of Cheating: Transparency and Non-Compliance in the Post-Cold War Era," in *A Future Arms Control Agenda: Proceedings of Nobel Symposium 118*, ed. Ian Anthony and Adam Daniel Rotfeld (Oxford, UK: Oxford University Press, 1999).

[4] Thomas C. Schelling and Morton H. Halperin, *Strategy and Arms Control* (Washington, DC: Pergamon-Brassey, 1985); and Dunn, "Arms Control Verification," 103.

[5] Tanya Ogilvie-White, "The IAEA and the International Politics of Nuclear Intelligence," *Intelligence and National Security* 29, no. 3 (2014): 323–40, https://doi.org/10.1080/02684527.2014.895591.

[6] Andrew J. Coe and Jane Vaynman, "Why Arms Control Is So Rare," *American Political Science Review* 114, no. 2 (May 2020): 342–55, https://doi.org/10.1017/S000305541900073X.

[7] Coe and Vaynman, "Why Arms Control Is So Rare," 347.

[8] In the early 1980s, U.S. experts were concerned that if Soviet inspectors visited American weapons factories, they would also collect sensitive intelligence information, citing an example where metal filings from the floor of an aircraft plant allowed the Soviet Union to gain valuable information about construction materials. Robert C. Toth, "Verification of Arms Pact May Open Spy Door," *Los Angeles Times*, Jan. 10, 1988, https://www.latimes.com/archives/la-xpm-1988-01-10-mn-34735-story.html.

[9] Nadia Kostyuk and Yuri M. Zhukov, "Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?" *Journal of Conflict Resolution* 63, no. 2 (February 2019): 317–47, https://doi.org/10.1177/0022002717737138.

stability,[10] coercion,[11] and crisis escalation,[12] far less attention has been paid to the possible effect on cooperation tools and agreement design.[13] Recent scholarship that does directly explore the intersection between emerging technology and agreement verification focuses almost entirely on the benefits for transparency without considering the potential for increased security risks.[14] At the same time, scholars have begun to explore how the spread and availability of technologies such as satellites have an effect on information asymmetries between the government and the public.[15] Such developments have implications for informational shifts in agreement design as well. Indeed, the potential for technology to affect treaty monitoring is recognized even in treaties themselves. Treaties like Open Skies and the Comprehensive Nuclear Test Ban, which go further than most in specifying which technologies will be used for monitoring, note that new technologies may be considered by the parties in the future.[16]

A closer consideration of possible changes in monitoring capabilities reveals several important implications for assessing the impact of technology on prospects for agreements. First, technology that allows for improvement in unilateral information collection — collection that can be conducted effectively without consent from the monitored state — will make formal agreements more likely by creating areas of potential cooperation where the security-transparency trade-off does not apply. Second, technology that allows for both greater control over specifically what information is collected through monitoring, and greater openness in revealing monitoring methods to the adversary, will decrease the severity of the trade-off. Having demonstrable control over collected information can mitigate the risk of additional security information being collected in the course of agreement monitoring and, as a result, make it easier for states to sign agreements. Conversely, technology that allows states to expand the scope of information collection, or makes it difficult for states to reveal how information collection works, will exacerbate the trade-off. Finally, technology that enhances a state's capability to conceal or deceive will make agreements less likely by creating a need for higher transparency to effectively monitor compliance, which will, in turn, create greater security costs.

Together, these key dimensions — unilateral monitoring, demonstrable control, and concealment — create a systematic and generalizable framework for assessing the possible effects of any new monitoring technology on arms control. This article investigates four emerging technologies that have some of the clearest applications in arms control monitoring: small satellites, drones, AI, and additive manufacturing (or "3D printing"). The analysis shows how technological changes affect both sides of the transparency-security trade-off, suggesting that agreements will be likely under some conditions and impossible in others. Perhaps counter-intuitively, more effective monitoring does not mean better prospects for arms control. Based on the assessment of specific technological developments presented in this article, the conclusion is a mixed one, with considerable pessimism. Even though capabilities such as small satellites and AI would allow for more effective verification, states may be less likely to sign agreements that utilize some emerging technology tools out of a fear that new security vulnerabilities will be revealed and exploited.

This article first builds on the theory of the transparency-security trade-off by identifying conditions under which technological change would be expected to affect the severity of the trade-off and by developing a framework for identifying implications for cooperation prospects. It then uses this framework to assess the possible effects of several

[10] Todd S. Sechser, Neil Narang, and Caitlin Talmadge, "Emerging Technologies and Strategic Stability in Peacetime, Crisis, and War," *Journal of Strategic Studies* 42, no. 6 (2019): 727–35, https://doi.org/10.1080/01402390.2019.1626725; Michael C. Horowitz, "Artificial Intelligence, International Competition, and the Balance of Power," *Texas National Security Review* 1, no. 3 (May 2018), https://doi.org/10.15781/T2639KP49; and Christopher F. Chyba, "New Technologies and Strategic Stability," *Daedalus* 149, no. 2 (Spring 2020): 150–70, https://doi.org/10.1162/daed_a_01795.

[11] Amy Zegart, "Cheap Fights, Credible Threats: The Future of Armed Drones and Coercion," *Journal of Strategic Studies* 43, no. 1 (2020): 6–46, https://doi.org/10.1080/01402390.2018.1439747.

[12] Caitlin Talmadge, "Emerging Technology and Intra-War Escalation Risks: Evidence from the Cold War, Implications for Today," *Journal of Strategic Studies* 42, no. 6 (2019): 864–87, https://doi.org/10.1080/01402390.2019.1631811.

[13] A recent review article on the effects of emerging technology on international politics notably lacks discussion about agreements or international institutions. Michael C. Horowitz, "Do Emerging Military Technologies Matter for International Politics?" *Annual Review of Political Science*, no. 23 (May 2020): 385–400, https://doi.org/10.1146/annurev-polisci-050718-032725.

[14] Graef and Kutt, "New Opportunities to Build Trust and Ensure Compliance."

[15] Erik Lin-Greenberg and Theo Milonopoulos, "Private Eyes in the Sky: Emerging Technology and the Political Consequences of Eroding Government Secrecy," *Journal of Conflict Resolution* 65, no.6 (2021): 1067–97, https://doi.org/10.1177/0022002720987285.

[16] Randy W. Bell, "CTBTO Science and Technology for a Safer World," in *International Cooperation for Enhancing Nuclear Safety, Security, Safeguards and Non-Proliferation–60 Years of IAEA and EURATOM,* Proceedings of the XX Edoardo Amaldi Conference, Accademia Nazionale Dei Lincei, Rome, Italy, Oct. 9–10, 2017, ed. Luciano Maiani, Said Abousahl, and Wolfango Plastino, vol. 206, Proceedings in Physics (Rome: Springer, 2017), 170, https://link.springer.com/book/10.1007/978-3-662-57366-2.

emerging technologies, highlighting in particular where a technology has countervailing effects along different dimensions. The conclusion discusses how this framework can empower analysis of both future developments and other potentially relevant technologies.

Monitoring Capability and the Transparency-Security Trade-Off

Information plays a dual role in arms control agreements. It can provide assurance of compliance or indicate violations, but it can also affect the balance of power between states. Classic arms control literature focused almost exclusively on the benefits of information for detecting cheating and the need for agreements to stipulate inspections when unilateral forms of information collection were insufficient to provide transparency.[17] Work that notes the role of national intelligence agencies in agreement verification has focused on the benefits of these tools for assuring compliance,[18] rather than on the security costs that both an opponent's intelligence capabilities and international monitoring agencies might create for the monitored state. More recent research has focused on the impact of agreement-related information on a state's relative military advantage. For example, Allison Carnegie and Austin Carson show that states hesitate to reveal that they have detected agreement noncompliance, when doing so will reveal secrets about their intelligence capabilities and will potentially forfeit a future military advantage.[19]

In the article "Why Arms Control is So Rare," authors Andrew Coe and Jane Vaynman focus directly on information dilemmas in agreements themselves.[20] They introduce the concept of the transparency-security trade-off, whereby information needed to monitor compliance also creates costs to a state's future security. However, Coe and Vaynman provide only preliminary ideas about the conditions under which the trade-off may be more or less severe, in terms of the degree to which marginal increases in transparency create security costs. The conditions they discussed focused on the nature of the states involved and on the characteristics of the capabilities that are being limited, but not on the different ways that monitoring itself can be carried out.

Building on this concept, the current article identifies three monitoring-related factors that are likely to affect the transparency-security trade-off, and in doing so the potential for reaching arms control agreements. First, the degree to which a technology enhances unilateral monitoring capabilities will determine whether the trade-off applies in particular cases. Second, the degree to which a technology alters the ability of states to demonstrably control the amount and quality of information collected can affect the severity of the trade-off. Finally, technological changes may affect not only the capacity to collect information about compliance but also how states conceal their activities, which in turn affects transparency needs in an agreement.

Changes in the way that monitoring is conducted, caused by innovation in the technology of information collection and information processing, are likely to affect the transparency-security trade-off, and in doing so, have an impact on when states come to an agreement.

The core logic of the transparency-security trade-off is that in order for states to prefer an arms control deal over a costly status quo — such as an arms race or conflict — an agreement needs to offer enough transparency into the behaviors of other states to be able to detect agreement violations, while maintaining enough secrecy such that their relative balance of power does not alter. These requirements are in tension, because greater

[17] Kenneth W. Abbott, "Trust but Verify: The Production of Information in Arms Control Treaties and Other International Agreements," *Cornell International Law Journal* 26, no. 1 (1993): 1–58, https://scholarship.law.cornell.edu/cilj/vol26/iss1/1; Lewis A. Dunn, "Arms Control Verification: Living with Uncertainty," *International Security* 14, no. 4 (Spring 1990): 165–75, https://www.jstor.org/stable/2538757; and Coit D. Blacker and Gloria Duffy, *International Arms Control: Issues and Agreements* (Stanford, CA: Stanford University Press, 1984). For a broader perspective on the costs and benefits of information, see also, Ronald B. Mitchell, "Sources of Transparency: Information Systems in International Regimes," *International Studies Quarterly* 42, no. 1 (March 1998): 109–30. https://www.jstor.org/stable/2600819.

[18] James M. Acton, "International Verification and Intelligence," *Intelligence and National Security* 29, no. 3 (2014): 341–56, https://doi.org/10.1080/02684527.2014.895592.

[19] Allison Carnegie and Austin Carson, "The Disclosure Dilemma: Nuclear Intelligence and International Organizations," *American Journal of Political Science* 63, no. 2 (April 2019): 269–85, https://doi.org/10.1111/ajps.12426.

[20] Coe and Vaynman, "Why Arms Control Is So Rare."

transparency can undermine secrecy. How much transparency is needed to ensure compliance can depend on a number of factors, including the physical nature of the capability or action being limited, what would constitute a militarily significant violation, and the potential costs of failing to detect a violation. Relatively *less* transparency is needed, for example, to observe military capabilities that are physically large. Relatively *more* transparency would be needed if a violation — such as secretly building a nuclear weapon — would have a very large effect on the future balance of power.

When states have sufficient transparency to be able to detect violations on their own, without any additional information provided or access granted by the other side, agreements with essentially no monitoring provisions are possible. This kind of "unilateral monitoring" capability can detect military secrets even without an arms control agreement. For example, satellites already collect information on an adversary's military bases. Using those images specifically to verify agreement compliance would not change what can be collected.[21] Agreements that rely on unilateral monitoring avoid the transparency-security trade-off because they do not introduce any new threats to a state's security.

If unilateral monitoring is insufficient to meet the transparency requirement, states will need agreements that allow them to collect additional compliance information. These kinds of agreements include extra monitoring tools that one state would not be able to use without the consent of the other state. On-site inspections are the best example of this type of tool because states need to willingly allow inspectors to access the relevant sites. Similarly, tools such as cameras or measuring equipment can only be installed with the monitored state's participation. As intrusive monitoring increases, the risks to security also increase. But the extent of that marginal increase in security risk can vary. If small increases in the intrusiveness of monitoring expose significant vulnerabilities, the trade-off is severe. Conversely, if increases in monitoring expose few vulnerabilities then the trade-off is mild. The more severe the trade-off, the more likely it is that states will prefer the status quo over signing a deal.

Effects of Changes in Monitoring Capabilities

When considering the monitoring capabilities themselves, several challenges emerge. First, the scope of agreements that rely on unilateral capabilities is limited by what those capabilities can detect. Any changes in those detection capabilities would expand the range of agreements that can be signed. The more that states can observe unilaterally, the more willing they will be to cooperate on particular arms control limitations. If a state can only observe large armaments, such as ships or missiles, those may be the only capabilities over which it is willing to negotiate. If observation capabilities were to change to make smaller objects detectable, then agreements about smaller armaments, which still do not rely on intrusive inspections, would be more likely. This could apply both to the types of military armaments that are being limited and to the extent of the limitations.

There are several ways in which unilateral monitoring can improve. First, there could be improvements that allow for the detection of ever-smaller items or behaviors. Second, observation can become more pervasive, allowing the state to detect changes over shorter periods of time. Third, if the costs of intelligence gathering are reduced, states can increase the volume of information that they can collect. These improvements can result from the same technology. For example, a new technology might enable a state to go from being able to see an adversary's military installation to observing vehicles next to it, and from seeing vehicles occasionally to being able to detect that they tend to arrive every Monday, and all at half the cost of the prior capability. Any technology that has applications in national intelligence would also have implications for arms control. In addition to improvements in national capabilities, advancements in monitoring tools provided by an international organization could enhance a state's ability to observe compliance without the acquiescence of the party being observed. The International Monitoring System of the Comprehensive Nuclear-Test-Ban Treaty is a good example. This system includes a range of sensors — seismic, hydroacoustic, infrasound, and atmospheric radionuclide — that allow it to monitor nuclear testing around the globe. The logic of technological effects on unilateral monitoring suggests that those emerging capabilities that allow for persistent and fine-grained observation from

[21] Some agreement provisions improve the capacity of unilateral monitoring by mandating that states cannot interfere with satellites or use concealment methods. While such measures may improve espionage capacity in that they allow intelligence agencies to devote fewer resources to treaty verification, they do not change the capabilities themselves. The "freeing up resources" factor also becomes less important as satellite capabilities become less scarce over time.

well outside a state's borders would make future arms control agreements more likely.

The second challenge is more complex. For agreements that need to rely on intrusive inspections to attain a sufficient level of transparency, the fundamental problem is that states will use information gathered in the process of verifying agreement compliance to then gain a military advantage. To some extent, this problem cannot be solved. When the very same information needed to verify compliance also creates vulnerabilities, the trade-off is immutable. For example, if an agreement reveals the locations of military bases for monitoring, that information itself also provides the adversary with a list of targets for a future military conflict.

However, some vulnerabilities can be mitigated by limiting what information inspections or other information-gathering tools can collect. This is the case when risk is associated with extra, non-agreement-related information that might be collected in the process of conducting agreement verification. For example, sensing equipment might be able to pick up information on capabilities beyond those being limited by a given agreement, or human inspectors might look around and observe other significant details at a site they are inspecting. Collecting extra information is of course perfectly rational from an adversary's point of view, and there is every reason to expect that espionage will happen if it is possible. U.S. and Soviet arms control inspection teams routinely had an intelligence component, and while neither side advertised this activity, both quietly accepted it as a part of the process.

Research on how to verify limits on specific capabilities seeks to solve precisely this security problem. For example, contemporary research and development on technologies for verifying limits on nuclear warheads has focused on making determinations while protecting weapon-design information, using approaches such as information barriers aimed at removing "sensitive information while providing as much data as possible."[22] Another approach has focused on "zero-knowledge proofs," which provide a way to confirm that two objects are the same without revealing their physical characteristics.[23] Some security costs can therefore be mitigated when there are ways to narrow the scope of observation to information on agreement compliance and little else.

Technological change will play a role in this dynamic if it affects the degree of demonstrable control over the quantity or quality of the information collected in the course of intrusive monitoring. A monitoring tool that provides a high degree of control creates an ability to demarcate the line between what will be revealed and what will be kept secret at whatever point that line is negotiated. Control might be achieved by limiting the amount or scope of the information that can be collected, or through an ability to collect information at a specified quality or level of granularity. For example, a technology that allows states to build a visual measurement tool with a range of fixed resolutions suggests a higher degree of control compared to a tool that can only be built with one resolution, or a tool that does not allow for a specified level to be set for different circumstances. Greater control might also be achieved through a technical ability to determine when or how frequently information can be collected. The ability to turn data gathering on and off is one example of control with regard to frequency. If a monitoring technology provides a high degree of control, then states will have greater assurance that security information beyond the scope of the agreement will be safe while more compliance-relevant information is revealed.

Control over information is only part of the challenge, however. In order to alleviate security concerns, states need to know what the other side is capable of collecting and what they have, in fact, collected in the process of agreement monitoring. In other words, there needs to be demonstrable proof that the agreed-upon level of precision and scope in information collection is both technologically possible to attain and is being implemented as agreed. Otherwise, states would have every reason to suspect that high-precision sensing tools are actually being used to collect information not relevant to the agreement. However, to assure a monitored state that a tool is only collecting designated data, a monitoring state might have to reveal details about how the tool works, which itself may reveal sensitive information about the monitoring state's capabilities and technological advancements. Using a well-known and even

[22] National Academies of Sciences, Engineering, and Medicine, *Nuclear Proliferation and Arms Control Monitoring, Detection, and Verification*, 100.

[23] Some recent research in this space departs from the "information barrier" approach because information barriers also feature problems for security risk due to cyber vulnerabilities such as backdoors or encryption weaknesses. On this challenge and research on physical cryptographic verification, see R. Scott Kemp et al., "Physical Cryptographic Verification of Nuclear Warheads," *Proceedings of the National Academy of Sciences* 113, no. 31 (2016): 8618–23, https://www.pnas.org/content/113/31/8618. On zero-knowledge proofs, see Alexander Glaser, Boaz Barak, and Robert J. Goldston, "A Zero-Knowledge Protocol for Nuclear Warhead Verification," *Nature*, no. 510 (2014): 497–502, https://doi.org/10.1038/nature13457; and Sébastien Philippe et al., "A Physical Zero-Knowledge Object-Comparison System for Nuclear Warhead Verification," *Nature Communications* 7, no. 12890 (2016), https://doi.org/10.1038/ncomms12890.

outdated technology for monitoring makes it easier for states to have common knowledge about the security risks that it might create.

Since demonstrable control is a concept being introduced here, a further illustration is helpful. Suppose the monitoring "technology" in question is a human inspector. It is possible to have a fair amount of control over where that person goes, when they arrive at a site, or how long they stay, but there is no control over that person's ability to turn his or her head. Any information that is within eyesight can be collected. This is in contrast to something like a mounted camera, where both the resolution and the line of sight can be controlled. The capacities of human vision are of course common knowledge and so the technology is demonstrable in that sense. But it is only partially demonstrable because even if the host state confiscates all the inspector's notes to check for espionage, there is no way to demonstrate what the inspector remembers.

Different emerging technologies may increase or decrease demonstrable control when it comes to agreement monitoring. If a new monitoring technology is itself the object of secrecy, or is poorly understood by an adversary, then demonstrable control will be low and uncertainty about possible security risks will increase. On the other hand, if either the nature of the technology or the steps taken to integrate it into monitoring efforts make it easy to demonstrate what information was collected, then uncertainty about potential intelligence vulnerabilities could be mitigated. Indeed, one interesting advantage of the monitoring systems for the Comprehensive Nuclear-Test-Ban Treaty — including both the global sensors and the on-site inspections — is that the collection methods and technical details of specific tools are well understood by member states, due both to widespread access to the technologies and to efforts by the Comprehensive Nuclear-Test-Ban Treaty Organization to communicate and even practice verification scenarios with member states.[24] Any assessment of the potential impact of a new technology should therefore investigate the degree to which the technology allows for *demonstrable* information collection.

The third challenge to consider is how an emerging technology affects not just monitoring capabilities but also a state's ability to conceal information. The prior two factors — unilateral monitoring and demonstrable control — largely considered the information question from the perspective of the state doing the monitoring. For concealment, it is helpful to assume the perspective of the monitored state. This state has an interest in hiding violations if it is indeed in noncompliance. Even if it is complying, the monitored state has an interest in hiding other security-related information. If the state's ability to hide violations improves, and both sides know this to be the case, then the monitoring state will require a higher minimum level of transparency in order to reach the same level of assurance that agreement terms are being followed. Agreements that were previously verifiable with unilateral means alone might now require intrusive inspections, and inspections might now need to be more persistent or involve greater access. Technological developments can improve the ability to hide violations by making the capability in question smaller, more portable, or more effectively shielded from observation by changing its appearance or other physical properties. Or, a technology may make it possible for violations to happen more quickly, increasing the possibility that they will go undetected.

While improvements in a state's ability to hide violations would make an agreement more difficult to sign, an emerging technology that improves a state's ability to conceal sensitive information that lies beyond the scope of the agreement would improve the prospects for a negotiated deal. Traditional concealment efforts have often involved physically covering some capabilities, placing them inside buildings out of sight, or moving them at night. More advanced concealment capabilities have included electronic interference, such as jamming the collection of signals intelligence. New technology tools might allow states to selectively block detection by creating information barriers, or even improved physical barriers, between weapons that are limited by the treaty and those that are not. Technology may also provide states with improved ways of creating misinformation, or creating a greater volume of it, essentially diluting the benefits that might come from intelligence gathering during agreement monitoring.

In general, improvements in concealment capabilities are a double-edged sword in terms of their effect on prospects for arms control agreements. A given technology could help to conceal violations, sensitive information, or both. Improved concealment of violations would make agreements less likely by driving up the transparency needs, while better concealment of sensitive information could make agreements easier to design by mitigating severe security trade-offs. It may be very difficult to discern which effect is greater. While it is possible that a technology will affect one kind of concealment more than the other, intuition suggests that most innovations would apply to both.

[24] Bell, "CTBTO Science and Technology for a Safer World."

Analytic Framework

The discussion above leads to a set of implications about the effect of emerging technology on the severity of the transparency-security trade-off and the ease of creating arms control agreements. First, improvements in unilateral monitoring capabilities can increase the number of cases that avoid the transparency-security trade-off and make arms control agreements more likely. Second, monitoring technology that provides greater demonstrable control over information decreases the severity of the trade-off and will make agreements more likely. By the same token, technology that diminishes either the degree of control or the ability to demonstrate the information that was collected to other parties increases the severity of the trade-off and will make agreements less likely. Third, technology that allows the monitored state to better conceal violations increases the minimum transparency level needed for cooperation and will make agreements less likely. And finally, technology that improves the monitored state's capacity to conceal security capabilities not limited by an agreement decreases the severity of the trade-off and will make agreements more likely.

Importantly, these implications do not operate in isolation. The same technological change that affects unilateral monitoring technology may also affect concealment capabilities. Thus, the effects of emerging technologies need to be evaluated along multiple pathways, which may have opposing effects. The analytic challenge is to estimate the magnitude of those effects and come to an overall assessment of the impact on prospects for cooperation. However, in some cases, there is simply not enough data to make a judgment on which direction will prevail. The implications outlined above provide a framework that can, even in cases of limited information, organize the assessment process by identifying the key factors to consider and the possible negative and positive effects. In this way, it allows us to avoid the mistake of only considering some impacts of a technology and not others, such as impacts on transparency but not on security. The framework also provides a means of revising assessments as more information about and experience with emerging technologies enters the picture, and it directs our attention to those elements of technological change that will matter for arms control.

Among the technologies assessed in the next section — small satellites, drones, AI, and additive manufacturing — no single definitive answer emerges as to whether the transparency-security trade-off will be mitigated or exacerbated as a consequence of new technology applications in the arms control context. At the same time, assessing new technologies using this framework does strongly indicate that while some technologies are indeed likely to improve prospects for cooperation, others may make it more difficult.

Assessing the Effects of Emerging Technologies

This section surveys several emerging technologies, identifying how they can be used to monitor arms control compliance and where that technology-enabled monitoring may create new security vulnerabilities. The particular set of technologies were selected for analysis to demonstrate the broad utility of the framework. Since not all of the key information trade-offs occur in every case, this range of technologies illustrates how each of the factors discussed above — unilateral monitoring, demonstrable control, and concealment — plays out in specific contexts.

The cases of small satellites and drones represent contemporary advancements of technologies that have been previously used for treaty monitoring and intelligence gathering and are, in that sense, the most likely to be used for similar purposes in the future. The AI case moves further afield from past treaty-monitoring experience but it engages with a technology that is at the center of extensive ongoing research on applications for information processing, including in intelligence. Finally, the additive manufacturing case shows how a technology with other primary uses may also have important implications for generating and collecting information. This case also serves to illustrate some of the paradoxes that emerge, including that a technology that seemingly makes it easier for states to build capabilities that are restricted by a given agreement also potentially enhances the ability to detect whether those violations are taking place.

These four cases notably vary in their overall implications for arms control agreements, from improving prospects for cooperation to hindering them. The analysis therefore allows us to investigate the pathways toward different possible outcomes, rather than focusing on a set of technologies that, for example, are all likely to have positive effects on agreements. While these particular cases are useful for illustrating the full range of information trade-offs and positive and negative implications, the framework is equally applicable to other cases as well. For example, robotics or blockchain technology (which is addressed briefly in the conclusion) would be useful to examine in a longer study.

Table 1: The impact of emerging technologies on different factors in arms control monitoring

	Small Satellites	Drones	Additive Manufacturing	Artificial Intelligence
Unilateral monitoring	**Significantly improved** capabilities and access for visual and other data	**Significantly improved**, but with some limits & risks in data collection	**Diminished** if weapons can be reconstituted; **Improved** due to cyber access to networked components	**Improved** due to speed & quantity of analysis; **Diminished** because unexpected failures create reliability concerns
Demonstrable control over collected information	Not intrusive, so generally n/a. Commercial sats **improve** prospects for enforcement by relying on public information	**Diminished** due to flexibility of collection and secrecy around tech	**Improved** due to digital nature of information	**Highly diminished** due to secrecy and high uncertainty about algorithms and effects of information disclosures
Concealment of violations	**Indirect** effect; insight into what can be seen makes it difficult to hide violations, but can improve concealment if it informs decoys	**Indirect** effect, similar to small sats	**Improved** due to small size and flexibility of production	**Improved** due to innovations for spoofing
Concealment of other capabilities	**Indirect** effect; lower ability to conceal means capabilities become open secrets & mitigates trade-off for other monitoring measures	**Indirect** effect, similar to small sats on lower ability to conceal, but information is less public	**Diminished** if tech is integrated into numerous applications; **Maintained or improved** if tech is isolated	Possibly **some improvement** due to spoofing or misinformation
Overall effect	Agreements more likely	Agreements more likely if used for unilateral monitoring, less likely for cooperative intrusive monitoring	Mixed, greater reliance on tech may improve likelihood of some agreements	Agreements less likely

Notably, the assessment of these four technologies is forward-looking. Apart from satellite technology, which has long been used for arms control monitoring, the discussion focuses on technologies that *may* be used for monitoring in the future, and are occasionally mentioned in that context in policy discussions or conferences, but are not currently an explicit part of arms control monitoring regimes. Table 1 provides an overview of the assessment of each technology. The sections below discuss the cases in greater detail, evaluating each technology's impact on unilateral monitoring, demonstrable control over information collection, and concealment.

Small Satellites

The first technology, satellites, is an extension of advancements that previously had a large effect on the transparency-security trade-off. During the Cold War, satellites made it possible to observe a greater amount of an adversary's capabilities. Today, satellites can be much smaller, more numerous, and provide both higher-resolution images and a wider range of other data.

In comparison to traditional satellites, which have a mass of over 1000kg, small satellites typically weigh less than 500kg. "Nanosatellites" include those that are even smaller, weighing between 1kg to 10kg, or under 27U.[25] The image-resolution capa-

[25] "CubeSats" are nanosatellites built within standard dimensions, where 10cm x 10cm x 11.35cm is defined as a "1U" CubeSat. Deployed CubeSats can be 1U, 3U, etc. and can weigh between about 1–40kg.

bilities of these satellites have continued to improve over time, and in 2020 one of the larger commercial imagery satellite companies, Planet Labs, made 50cm imagery resolution available to consumers. Some companies are planning to offer 10cm resolution within the next decade.[26] Whereas in the past the U.S. government had placed restrictions on the resolution of commercially available images, since 2019 the limits have been lifted to a large degree, both with regard to resolution and other types of imaging, such as nighttime, radar, and infrared.[27] What restrictions remain are effectively meaningless from an intelligence perspective because non-U.S.-based companies are not subject to them.

In addition to capturing images, small satellites can be equipped with other kinds of sensors, such as spectrometers to measure soil materials, water abundances, pollutants, and hazardous gases, and infrared sensors for nighttime imaging and temperature mapping.[28] Sensing tools like synthetic aperture radar and hyperspectral imaging will become more available in commercial applications in the near future.[29] Unlike traditional communications satellites, many small and nanosatellites are launched into low earth orbit at an altitude of 500km to 2,000km. After two to three years, they drop out of orbit and burn up in the atmosphere. Early CubeSats were launched into space on Russian rockets, but today American, European, and other launch providers are widely available. However, launch remains a key bottleneck, expense, and source of risk for satellite providers.[30]

Nanosatellites are the fastest growing area of small satellite development and are being launched increasingly by private companies rather than governments. They allow for near real-time observation around the globe. More than 300 such satellites were launched in 2017 alone with predictions into 2025 rising to well above 500 per year.[31] As of April 2021, there were nearly 1,000 operational nanosatellites in orbit. Around 80 percent of nanosatellites are owned by companies and universities, with only about nine percent owned by militaries and space agencies. While the United States has launched the majority of nanosatellites, 75 other countries have nanosatellites as well.[32] Some of the well-known images from commercial satellites give a sense of the level of detail that can be picked up nearly in real time. For example, in summer 2020, Planet Labs posted images of the “Black Lives Matter” mural on the ground of a city block in Washington, DC, the day it was painted. Nanosatellites have also been used to assess hurricane damage and identify pasture for livestock.[33]

When it comes to arms control agreements, small satellites will improve unilateral monitoring capabilities by giving states an affordable way to gather more imagery across greater areas for longer periods of time. States could of course use this technology for general intelligence collection, and indeed they already do.[34] High-resolution persistent monitoring by satellites makes it more difficult for states to conceal capabilities. So whether it is for spying or verifying compliance, the threats to the security of a state that is being observed do not change when satellites are used to verify a specific compliance commitment. From the point of view of the intelligence community, formal arms control agreements were initially preferable because receiving voluntary information provided by the

[26] Alex Wilhelm, "Satellite Imagery Startup Albedo Closes $10M Seed Round," *TechCrunch*, April 22, 2021, https://techcrunch.com/2021/04/22/satellite-imagery-startup-albedo-closes-10m-seed-round/.

[27] David Schneider, "U.S. Eases Restrictions on Private Remote-Sensing Satellites," *IEEE Spectrum*, July 1, 2020, https://spectrum.ieee.org/tech-talk/aerospace/satellites/eased-restrictions-on-commercial-remote-sensing-satellites.

[28] "Home Page," Nanosats Database, Accessed May 4, 2021, https://www.nanosats.eu/.

[29] Synthetic aperture radar emits an electromagnetic signal and measures the bounce back and scatter from features on earth to create an image. It provides key advantages in being able to collect images through cloud cover and at night. For a good overview, see "SAR Overview," Jet Propulsion Laboratory, California Institute of Technology, Accessed Sept. 13, 2021, https://nisar.jpl.nasa.gov/mission/get-to-know-sar/overview/. Hyperspectral imaging uses hundreds of wavelengths across the electromagnetic spectrum to create images. It has been used in agriculture, mining, and environmental science to detect status of crops, composition of mining materials, etc. Previously, hyperspectral imaging was primarily done via drones, but applications for satellites are planned by both government and commercial actors. See for example, Adam Keith, "Is Hyperspectral the Next Earth Observation Frontier?" *SpaceNews*, March 30, 2019, https://spacenews.com/op-ed-is-hyperspectral-the-next-earth-observation-frontier/.

[30] Jamie Smyth, "Small Satellites and Big Data: A Commercial Space Race Hots Up," *Financial Times*, Jan. 23, 2018, https://www.ft.com/content/32d3f95e-f6c1-11e7-8715-e94187b3017e.

[31] For 2017 numbers, see Jeff Foust, "New Companies Needed to Maintain Small Satellite Market Growth," *SpaceNews*, Jan. 31, 2018, https://spacenews.com/new-companies-needed-to-maintain-small-satellite-market-growth/. For predictions, see "Nanosatellite Launches with Forecasts," Nanosats Database, accessed May 4, 2021, https://www.nanosats.eu/.

[32] "Home Page," Nanosats Database.

[33] Smyth, "Small Satellites and Big Data."

[34] "NGA's Primary Commercial Imagery Delivery System Now Includes Small Satellites," National Geospatial-Intelligence Agency, Public Release Number 20-704, Nov. 5, 2020, https://www.nga.mil/news/NGAs_primary_commercial_imagery_delivery_system_no.html; and Sandra Erwin, "NGA Wants Faster Access to Commercial Geospatial Data" *SpaceNews*, Jan. 12, 2021, https://spacenews.com/nga-wants-faster-access-to-commercial-geospatial-data/.

adversary and having an agreement that the adversary would not hide relevant capabilities from satellites eased the burden on intelligence resources. When satellites were expensive and limited in number, having an agreement possibly improved intelligence gathering capacity overall, and in doing so created some increased security risks for the target state, though only indirectly.

Today, with plenty of satellite capabilities to go around, an agreement would be far less likely to create a resource trade-off with other intelligence collection needs. As nanosatellites become less expensive, and satellite imagery becomes less of a limited resource, agreements relying on these measures for monitoring may become even easier to conclude because they will require even less voluntary information from an adversary.

Since satellites are used to collect information from outside a target state's borders, the issues of demonstrable control do not arise in the context of a transparency-security trade-off. But there are some key benefits of advances in satellite technology for generating demonstrable information that are worth noting. A key problem with using national technical means or any espionage tools to detect agreement violations arises when a state has to reveal that information in order to confront the violator, to garner support from allies and international organizations, or to convince domestic audiences that a particular response is necessary.[35] If states reveal information collected through intelligence capabilities, an adversary may learn enough to be able to deny that type of collection in the future, both in that particular context and possibly more broadly as well, given that intelligence methods are used across a range of efforts. Because of the need to protect sources and methods, claims of arms control violations based on intelligence often have the flavor of "just trust us." In contrast, relying on commercially available satellite data would make it easier for states to demonstrate their findings to other actors. This would be true even if violations were initially discovered through sophisticated national reconnaissance satellites but can be sufficiently backed up by commercial data. Non-governmental experts have increasing access to imagery, so the analytic burdens of detecting violations may also decrease due to crowdsourcing or citizen verification.[36] The higher degree of demonstrable information provided by emerging satellite technology can therefore make agreement enforcement easier, improving incentives for cooperation.

Finally, small-satellite technology only indirectly applies to concealment capabilities. Nevertheless, there are several ways in which the technology may still affect a state's ability to hide violations and other capabilities. When a monitored state lacks access to advanced satellite capabilities, or even to information about them, it is more difficult to intentionally hide violations. The state may want to conduct a banned activity or move a treaty-limited weapons system, but uncertainty about what the other side can and cannot observe may either deter that violation attempt in the first place, or allow the other side to detect it. Better knowledge about satellite capabilities would make it easier to identify gaps in observation and exploit them to conceal violations. This dynamic has played out in past cases. For example, during the Cold War, the capabilities of national reconnaissance satellites were closely guarded secrets. U.S. verification of arms control agreements relied in part on the Soviet Union being unable to detect when satellites were passing overhead or what information those satellites could capture. In 1979, the United States was worried that the Soviet Union had acquired secret details about U.S. reconnaissance satellites, which would allow the Soviet Union to implement more effective deception and denial, degrading the U.S. ability to monitor the Strategic Arms Limitation Talks (SALT) II accord. Congressional leaders questioned whether the reliance on "national technical means" laid out in the treaty would still be sufficient after the disclosures.[37]

Today, adversaries may still not fully know the capabilities of advanced national reconnaissance satellites, but the capabilities of commercial small satellites can be more readily accessed. The monopoly that the U.S. government previously held on high-quality satellite images has largely eroded.[38]

[35] Carnegie and Carson, "The Disclosure Dilemma."

[36] Christopher W. Stubbs and Sidney D. Drell, "Public Domain Treaty Compliance Verification in the Digital Age," *IEEE Technology and Society Magazine* 32, no. 4 (2013): 57–64, https://doi.org/10.1109/mts.2013.2286432.

[37] Richard Burt, "Arms Treaty: How to Verify Moscow's Compliance," *New York Times*, March 21, 1979, https://www.nytimes.com/1979/03/21/archives/arms-treaty-how-to-verify-moscows-compliance-laying-worries-to-rest.html?searchResultPosition=27. In 1978, the U.S. Defense Intelligence Agency had identified an increase in Soviet efforts to avoid detection and a decline in intelligence collected by the KH-11 imagery intelligence satellite system. A former CIA officer was later arrested for selling a classified manual on the system to the Soviet Union. For this example and more on satellite technology effects on Cold War intelligence, see Aaron Bateman, "Technological Wonder and Strategic Vulnerability: Satellite Reconnaissance and American National Security During the Cold War," *Journal of Intelligence and CounterIntelligence* 33, no. 2 (2020): 328–53, https://www.tandfonline.com/doi/full/10.1080/08850607.2019.1703926.

[38] Amy Zegart and Michael Morell, "Spies, Lies, and Algorithms: Why U.S. Intelligence Agencies Must Adapt or Fail," *Foreign Affairs* 98, no. 3 (May/June 2019): 85–96, https://www.foreignaffairs.com/articles/2019-04-16/spies-lies-and-algorithms.

Commercial images from non-U.S.-owned satellites are available to both non-U.S. countries and private actors.[39] The effect of this technology diffusion is that a state being monitored — or spied on — could have a pretty good idea of the kind of information that its adversary can collect. On the one hand, this knowledge may improve the ability to hide both violations and non-treaty limited capabilities by informing more sophisticated concealment methods, including decoys that mimic physical properties that advanced satellites can detect.[40] This kind of response could lead to skepticism in arms control and demands for greater transparency, potentially undermining agreements in ways quite similar to the U.S.-Soviet example from 1979. On the other hand, the ubiquity of a significant baseline of satellite monitoring information may serve to deter more violations because the reach of emerging capabilities will be readily apparent, demonstrating that concealment of violations is likely to be ineffective. It may also mitigate the monitored state's concerns that intrusive monitoring methods (such as inspections) will reveal sensitive information beyond the scope of the treaty. The location of a base, or even details about deployments there, are no longer a security vulnerability stemming from it being an inspection site because satellite imagery can show that this information is not a secret in the first place.

Developments in small satellite technology, therefore, have at least three implications for arms control agreements and the forms those agreements take. First, states will be more likely to sign agreements that do not include dedicated monitoring and verification provisions because transparency requirements will be addressed effectively through unilateral monitoring, which does not change the security risks faced by the monitored state. Here, better spying makes cooperation more likely. Second, the benefits of public satellite data may also provide assurance that enforcement of an agreement will be easier, and so will make states more willing to cooperate. Third the effects of emerging satellite technology on the ability of states to conceal their capabilities are likely to be mixed: Small satellite technology may dampen prospects for agreements if it informs counterintelligence efforts and it will increase cooperation where it reveals the futility of trying to maintain secrecy.

Drones

Technologically advanced states are developing drones for military purposes that range from carrying out attacks to conducting various forms of surveillance. Advances in surveillance capabilities are most relevant to arms control. One can imagine drones being used primarily to unilaterally monitor agreements, but they could also be used, at least theoretically, as accepted tools in intrusive verification at locations within a state's sovereign territory. Such capabilities could potentially be useful for tracking mobile capabilities when highly responsive monitoring is needed and mutually agreed upon for an important moment, such as for a weapons test or an exercise, but in-person inspections would be difficult to arrange or limited in capacity.

When it comes to gathering information, drones have particular advantages in being highly precise, capable of real-time tracking, and relatively inexpensive. Compared to satellites, drones can provide higher resolution imagery. They also have longer ranges and offer better fuel economy than human-piloted aircraft. Drones can be designed to "loiter" in particular areas, collecting high-quality, near real-time information for periods longer than a human would be able to sustain, or than a satellite would be able to cover due to its movement along an orbit. Further advantages over other kinds of surveillance include being able to access areas that are difficult for human pilots to operate in, such as very high altitudes.[41]

Recent innovations in drone technology for surveillance include "swarms" and ultra-high speeds. Swarms are made up of miniature drones moving in a coordinated, semi-autonomous way. Swarms could provide flexible and highly precise information collection options. Coordinated swarms of small sensing vehicles could improve detection of other difficult to observe mobile capabilities, such as submarines.[42] The U.S. Defense Advanced Research Projects Agency (DARPA) "Gremlins" program is developing swarms of small drones that can be air-launched from a larger airborne vehicle, like a bomber or cargo plane, use an array of sensing technologies to collect and communicate information, and then be recovered back into the larger aircraft. This capability would allow for highly flexible and

[39] Christopher A. Bidwell and Bruce W. MacDonald, "Emerging Disruptive Technologies and Their Potential Threat to Strategic Stability and National Security," Federation of American Scientists, September 2018, 30, https://fas.org/wp-content/uploads/media/FAS-Emerging-Technologies-Report.pdf.

[40] Rémy Hémez, "To Survive, Deceive: Decoys in Land Warfare," *War on the Rocks*, April 22, 2021, https://warontherocks.com/2021/04/to-survive-deceive-decoys-in-land-warfare/.

[41] "China Tests Spy Drones in Near Space 'Death Zone': Report," *NDTV.com*, Oct. 31, 2017, https://www.ndtv.com/world-news/china-tests-spy-drones-in-near-space-death-zone-report-1769303.

[42] Bidwell and MacDonald, "Emerging Disruptive Technologies and Their Potential Threat to Strategic Stability and National Security."

precise information-gathering while keeping expensive and detectable platforms at a safe distance.[43] Higher speed capabilities could also improve flexibility and responsiveness in monitoring. A hypersonic drone or intelligence, surveillance, and reconnaissance vehicle could be developed by 2030. Such a high-speed drone would be better able to enter and exit another state's territory to collect information without being detected or shot down.[44]

Using drones for unilateral monitoring could have benefits, but this possible application is also limited by the fact that, like manned aircraft, this capability would have to be explicitly sent somewhere at a particular time. The most likely use might therefore be for checking specific areas of concern, such as a test launch, rather than for doing persistent monitoring to track changes over longer periods of time. Using autonomous vehicles for extensive monitoring requires the adversary's cooperation in order to be effective. In cases where satellite or high-altitude imagery is not sufficient, a target state could give permission for drones to fly into its territory to monitor weapons deployments or troop movements. Without cooperative agreement from both parties accepting the use of drones for monitoring, efforts to do so unilaterally would simply be spying, and the target state would have every incentive to take countermeasures. Some arms control agreements ban states from interfering with "national technical means" for monitoring without specifically defining the term, but it is generally accepted to mean satellite observation, not observation with drones or planes. Though most advanced drones are difficult to detect and intercept, there is still some risk that a drone will be shot down. Costs are relatively low because a pilot's life is not at stake, but an incident could escalate tensions or undermine diplomacy. For example, in 2019 Iran shot down a U.S. Global Hawk (a large and expensive drone surveillance system) and targeted but failed to take down a Reaper drone. The Global Hawk incident led to a discussion of escalation and tension over whether it had occurred over Iranian or international territory.[45]

The security risks — either real or perceived — that stem from cooperative monitoring with drones will likely outweigh the transparency benefits.

Explicitly including drones as part of cooperative monitoring provisions in an agreement is appealing. Using drones to monitor compliance without the risk of attack or without denial and deception employed by the target state would have significant transparency benefits. But using drone technology would also pose heightened risks to security because it creates a low degree of demonstrable control. The use of drones could make it difficult for a state to demonstrate that it is limiting its observations to predesignated areas, or to demonstrate how often it is gathering information and at what level of detail. Compared to human inspectors or piloted aircraft taking photos under the supervision of representatives from both states, it would be easier for a drone (or a swarm of mini-drones) to alter its path to collect sensitive intelligence. The speed and flexibility that make this technology so effective for surveillance and reconnaissance also make it particularly well suited for secretly collecting information beyond the scope of an agreement. In principle, the monitoring state might be able to show that its drone data-collection capabilities, flight paths, and control algorithms were set up to reflect negotiated limits for observation. But doing so in a convincing way would reveal capabilities about the technology itself, both for drones and AI that may be used to guide them. This, in turn, would increase the security risk for the monitoring state, making it an unacceptable solution.

The security risks — either real or perceived — that stem from cooperative monitoring with drones will likely outweigh the transparency benefits. It is telling that past use of even piloted aircraft in arms control, with observable flight paths and mutually agreed upon sensor equipment, led to concerns about an adversary gaining intelligence advantages. The Open Skies Treaty permitted reconnaissance

[43] Paul J. Calhoun, "Gremlins," Defense Advanced Research Projects Agency, accessed May 5, 2021, https://www.darpa.mil/program/gremlins; and "Gremlins: Airborne Launch & Recovery of Unmanned Aerial Systems," DARPAtv, video recording, May 11, 2018, https://www.youtube.com/watch?v=Bvf9v4EHovY.

[44] Kris Osborn, "U.S. Air Force Chief Scientist Says Hypersonic Weapons Ready by 2020s," *The National Interest*, April 27, 2016, https://nationalinterest.org/blog/the-buzz/us-air-force-chief-scientist-says-hypersonic-weapons-ready-15962.

[45] Lily Hay Newman, "The Drone Iran Shot Down Was a $220M Surveillance Monster," *Wired*, June 20, 2019, https://www.wired.com/story/iran-global-hawk-drone-surveillance/.

flights over the other state's territory to gather information on military activities. The United States withdrew from the agreement in November 2020.[46] Though it drew skepticism from many experts, one of the claims that became salient in the political debate was that, under the treaty, Russia was gaining intelligence advantages, including on U.S. critical infrastructure.

In sum, drones offer benefits for unilateral monitoring, though with some caveats with regard to limited scope and increased risks. Using drones in cooperative monitoring agreements could put that limited scope to good use by addressing areas that states find most challenging to observe, such as mobile capabilities. But, the technology brings with it a low degree of demonstrable control, indicating that any transparency benefits gained in cooperative monitoring will also come with serious concerns about security threats. Finally, for a state seeking to conceal its violations or capabilities, access to drone technology does not, in itself, affect those efforts, although it could indirectly do so by informing the state how to develop countermeasures, following the same logic as discussed above for satellites.

Artificial Intelligence

AI technology involves the use of machines or computers to do tasks that one would normally think of as requiring human thought. The line between "automation" and "artificial intelligence" is not clear-cut, but AI usually refers to capabilities that can take in information and adapt their own analysis or actions without human intervention. AI algorithms use data to learn rules, patterns, and decisions that the algorithms can reapply to assess new information and take actions in response. Popular examples include computers that have learned to win at chess and the more intricate and complex game of Go.[47] The United States, as well as China, Russia, and other states, are investing heavily in AI technology for both civilian and military purposes.[48] It is clear that the capabilities of this technology will improve rapidly in the near future.

AI may be used to assist arms control monitoring and verification by increasing the efficiency of information processing in order to detect violations. In this way, it intersects directly with the two information-gathering technologies already discussed. Today, intelligence capabilities suffer from too much information rather than too little, making analytical capacity a major constraint.[49] The problem applies to observing state behavior in general and to verifying compliance if there is an agreement to govern some part of it. As discussed below, AI has tended to be more appropriate for analyzing repeated, rather than rare, events. Though instances of treaty violations are relatively rare, plenty of other information within the arms control context, such as patterns in military behavior and deployments, are indeed of that repeated variety. In this sense, AI might help to detect something like a missile test (either in accordance with or in violation of an agreement) based on data about preparations, construction, or communications. AI tools can also be applied to assess information gathered from intrusive verification methods like inspections or automatic detection with mounted sensors.

In general, AI systems work by first "training" the system based on observed data and then directing it to identify and classify new information. The types of algorithms and processes used at both the training stage and the new data stage vary, with different approaches to how the systems observe and classify information. Studies have shown that developments in AI are increasingly able to compete with human vision when it comes to classifying visual objects.[50] "Computer vision" involves classification, recognition, and detection. Driverless cars are a well-known commercial application. New research focuses on developing algorithms to improve the accuracy and computational efficiency of these "vision" processes, as well as ways

[46] Kingston Reif and Shannon Bugos, "U.S. Completes Open Skies Treaty Withdrawal," *Arms Control Today*, December 2020, https://www.armscontrol.org/act/2020-12/news/us-completes-open-skies-treaty-withdrawal.

[47] Paul Mozur, "Google's AlphaGo Defeats Chinese Go Master in Win for A.I.," *New York Times,* May 23, 2017, https://www.nytimes.com/2017/05/23/business/google-deepmind-alphago-go-champion-defeat.html.

[48] Ashwin Acharya and Zachary Arnold, "Chinese Public AI R&D Spending: Provisional Findings," Center for Security and Emerging Technology, December 2019, https://doi.org/10.51593/20190031; Margarita Konaev, "Thoughts on Russia's AI Strategy," Center for Security and Emerging Technology, Oct. 30, 2019, https://cset.georgetown.edu/article/thoughts-on-russias-ai-strategy/; Nikolai Markotkin and Elena Chernenko, "Developing Artificial Intelligence in Russia: Objectives and Reality," Carnegie Moscow Center, May 8, 2020, https://carnegie.ru/commentary/82422; Justin Doubleday, "New Analysis Finds Pentagon Annual Spending on AI Contracts Has Grown to $1.4B," *Inside Defense*, Sept. 24, 2020, https://insidedefense.com/insider/new-analysis-finds-pentagon-annual-spending-ai-contracts-has-grown-14b.

[49] Aaron F. Brantly, "When Everything Becomes Intelligence: Machine Learning and the Connected World," *Intelligence and National Security* 33, no. 4 (2018): 562–73, https://doi.org/10.1080/02684527.2018.1452555.

[50] Anh Nguyen, Jason Yosinski, and Jeff Clune, "Deep Neural Networks Are Easily Fooled: High Confidence Predictions for Unrecognizable Images," *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, (2015): 427–36, https://www.cv-foundation.org/openaccess/content_cvpr_2015/html/Nguyen_Deep_Neural_Networks_2015_CVPR_paper.html.

to track subjects as they move.[51] The need for real-time, highly accurate analysis in 3D for consumer vehicles is likely a higher bar than what would be needed to detect militarily useful information about an adversary's activities, troop movements, or capabilities.

AI applications can provide significant advances in unilateral monitoring capability. With satellite technology, states are already able to collect vast amounts of visual data on other countries. Improvements in AI technology could make it possible to analyze that visual data at greater speeds for very specific goals. As image-collection technology develops, the bottleneck is increasingly in humans having to look at the data. The U.S. National Geospatial Intelligence Agency has invested in AI projects intended to assist analysts with routine tasks, streamline analysis, identify biases, and work with large datasets.[52] Robert Cardillo, the director of the National Geospatial Intelligence Agency, has discussed his interest in AI and automation and his goal of using computers, rather than analysts, to assess images.[53] Dawn Meyerriecks, CIA deputy director for technology development, stated in 2017 that the agency has numerous AI-related projects, and that it intends to use the technology to improve intelligence collection.[54] In arms control, tracking the numbers and locations of mobile missiles has always been a challenge for treaty verification efforts. Greater amounts of imagery combined with automated image identification could help solve this problem. AI tools can also be used to enhance non-image-based detection, such as identifying small nuclear tests among the vast array of seismic data collected as part of the Comprehensive Nuclear-Test-Ban Treaty monitoring system.[55] Importantly, innovations in this space are not limited to the United States, and other states are likewise seeking to use AI for tackling data, including for intelligence purposes.[56]

The combination of persistent surveillance by satellites with fast analysis by AI algorithms creates an improved ability to detect changes in an adversary's capabilities, detect movements of military units or weapons, track mobile missiles, or identify military production facilities.[57] Additionally, the rise in digital connections, including both communications and networked devices, means that intelligence collection can draw on a broader range of sources with a higher level of detail. Data collected by nearly all forms of intelligence (e.g., signals intelligence, measurement and signature intelligence, cyber intelligence, and social media intelligence) is growing almost exponentially. While the use of automation and computational analysis in intelligence is not new — it dates back to early computers in the post-World War II era and the growth of the National Security Agency as an intelligence agency — contemporary advancements in AI will likely alter multiple aspects of information analysis.

While AI has the potential to improve unilateral monitoring in important ways, the benefits may also be somewhat overstated. AI systems are brittle. They can vacillate between very high and very low levels of accuracy and have been shown to fail in unpredictable ways.[58] Pattern-recognition AI, or deep neural networks, are particularly prone to failure when encountering unfamiliar data. Researchers note that it is not that the AI systems fail, but that they fail in strange ways, making mistakes that designers did not imagine were possible.[59] In addition, the quality and amount of training data can vary, which will impact AI capabilities. Training data may also introduce bias in ways that are not anticipated by the AI designers.

In the context of cooperative monitoring, AI-en-

[51] Denis Tomè et al., "Deep Convolutional Neural Networks for Pedestrian Detection," *Signal Processing: Image Communication*, no. 47 (September 2016): 482–89, https://doi.org/10.1016/j.image.2016.05.007; and Brunetti et al., "Computer Vision and Deep Learning Techniques for Pedestrian Detection and Tracking: A Survey," *Neurocomputing*, 300, (2018): 17–33, https://doi.org/10.1016/j.neucom.2018.01.092.

[52] For details on 2017 contracts, see Loren Blinde, "NGA Awards Four Contracts to Enhance Artificial Intelligence and Automation," *Intelligence Community News*, Feb. 16, 2017, https://intelligencecommunitynews.com/nga-awards-four-contracts-to-enhance-artificial-intelligence-and-automation/.

[53] Jenna McLaughlin, "Artificial Intelligence Will Put Spies Out of Work, Too: Secret Mapping Agency Aims to Automate the Bulk of Its Work," *Foreign Policy*, June 9, 2017, https://foreignpolicy.com/2017/06/09/artificial-intelligence-will-put-spies-out-of-work-too/.

[54] Paul Handley, "Data Swamped US Spy Agencies Put Hopes on Artificial Intelligence," *Phys.org*, Sept. 9, 2017, https://phys.org/news/2017-09-swamped-spy-agencies-artificial-intelligence.html.

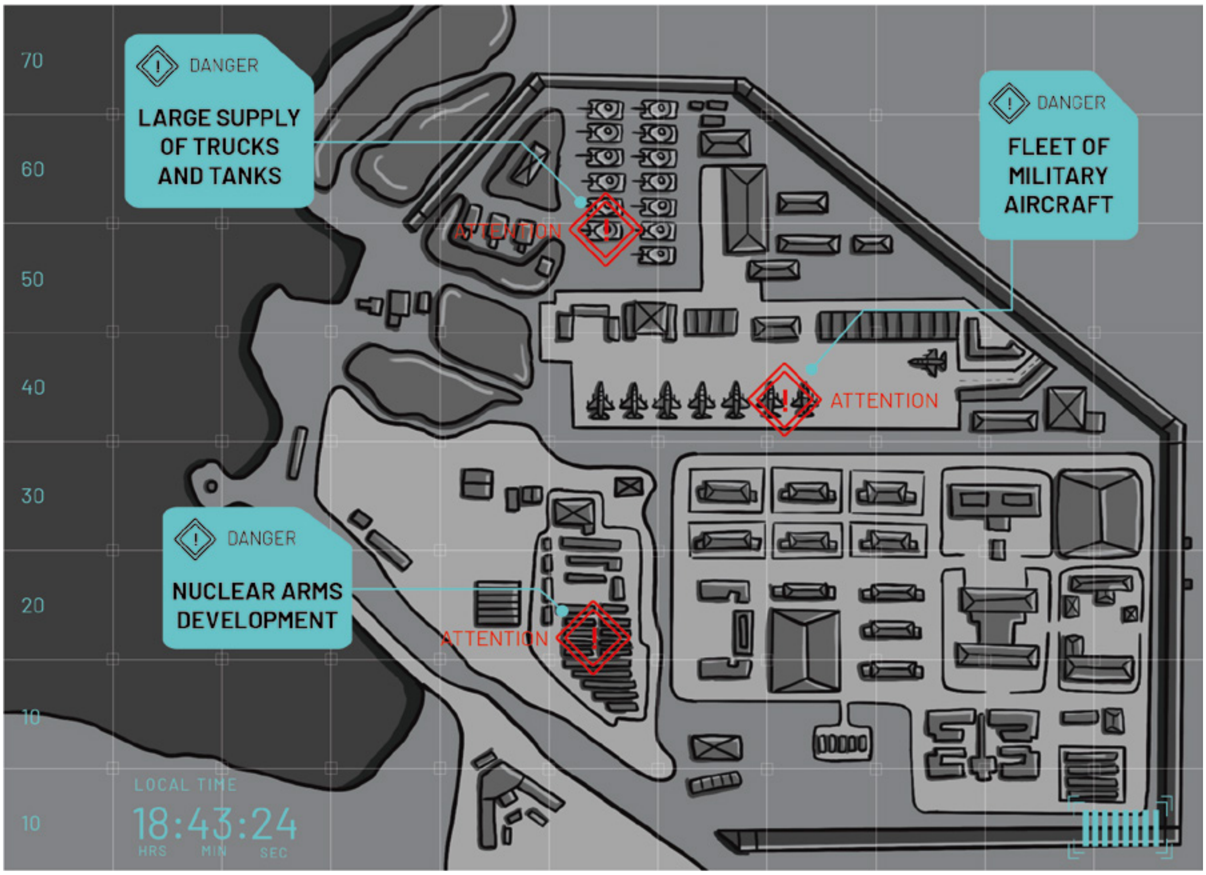
[55] National Academies of Sciences, Engineering, and Medicine, *Nuclear Proliferation and Arms Control Monitoring, Detection, and Verification*, 102.

[56] Pierre Tran, "French Intelligence Agency Wants AI to Help Sort Masses of Raw Data," *Defense News*, Feb. 5, 2018, https://www.defensenews.com/global/europe/2018/02/05/french-intelligence-agency-seeks-ai-to-support-analysts/; and Yaakov Lappin, "Artificial Intelligence Shapes the IDF in Ways Never Imagined," *The Algemeiner*, Oct., 16, 2017, https://www.algemeiner.com/2017/10/16/artificial-intelligence-shapes-the-idf-in-ways-never-imagined/.

[57] Bidwell and MacDonald, "Emerging Disruptive Technologies and Their Potential Threat to Strategic Stability and National Security."

[58] Kalev Leetaru, "We Must Recognize Just How Brittle and Unpredictable Today's Correlative Deep Learning AI Is," *Forbes*, June 24, 2019, https://www.forbes.com/sites/kalevleetaru/2019/06/24/we-must-recognize-just-how-brittle-and-unpredictable-todays-correlative-deep-learning-ai-is/?sh=510631a15bb1.

[59] Douglas Heaven, "Why Deep-Learning AIs Are so Easy to Fool," *Nature*, Oct. 9, 2019, https://www.nature.com/articles/d41586-019-03013-5.



abled systems are likely to provide a low degree of demonstrable control, thereby increasing concerns that sensitive security information could be collected in the course of agreement monitoring. AI tools such as computer vision could be integrated into systems like continuous monitoring to detect and categorize objects moving in the field of a camera, verifying characteristics that are relevant for a particular arms control rule. It could also play a role in the sensors and measurement equipment used by inspectors. However, these advances may also heighten fears of espionage. Monitored states may fear that AI-enabled data processing tools will make it more difficult to discern what amounts or quality of information are being collected. Even if AI is not used in the inspections themselves, the diffusion of AI in data analysis for intelligence could lead to concerns that even limited data or an incomplete detail would, with the help of AI-enabled analysis of multiple sources, allow the monitoring state to gain a security advantage. Whereas before, the monitored state might have had a good sense of what needs to be hidden to maintain its security, the adversary's greater integration of AI would make it less clear which information presents a security risk. The marginal cost to security posed by intelligence information that might be collected during an arms control inspection would be more difficult to assess and potentially large, suggesting a severe transparency-security trade-off.

Even if, in reality, no extra security-relevant information is being collected, target states may continue to have concerns about that prospect due to the difficulty of making AI capabilities demonstrable. Other states' AI capabilities are not widely known, and AI algorithms are themselves often considered as highly sensitive information. Demonstrating the details of AI capabilities to reassure the target state could create security vulnerabilities for the monitoring side. Such vulnerabilities could stretch well beyond the specific arms control application, revealing the state of scientific research and technical know-how. As AI becomes increasingly integrated across numerous military applications and commercial sectors, sensitive information about one application could compromise others. AI technology also inherently has limited demonstrability, not only for the target state, but also for the monitoring state itself. The algorithms of the learning process in neural networks are themselves a black box, and outcomes cannot be adjusted with changes in a line of code or even explained.[60]

AI's potential effects on concealment raise perhaps the greatest amount of unanswered questions and concerns. The vulnerability is two-fold. States could use knowledge of AI weaknesses to exploit algorithms, or use AI capabilities to generate misleading information, both of which can make concealment of agreement violations or other capabilities more effective. Looking at each of these scenarios suggests that a pattern of innovation and response will create uncertainty about whether the technology will privilege detection or concealment at a given point in time.

Innovations in Generative Adversarial Networks (GANs) are likely to have a significant impact on both avoiding detection and creating false information. A GAN model essentially pits two AI networks against one another. One generates new data, such as an image, based on a training set, and the other tries to discriminate whether the image is fake or real, or in other words whether it was generated from a model or came from real training data. The competition between these two systems allows both to iteratively improve.[61] Research with GANs is expanding rapidly. For example researchers are able to generate 3D models of objects based on flat images, even with the presence of noise and lighting variations.[62] The GANs approach is particularly useful when there are limits in the size or quality of the training data.

As AI technology becomes more integrated and more accessible to different actors, a state could exploit weaknesses specific to AI technology to avoid detection of agreement violations or military capabilities in general. Research in the civilian sector has repeatedly shown that AI can be relatively easy to dupe. For example, researchers have shown that deep neural networks used to classify images can be "fooled" into making high-confidence assessments of images that are incorrect.[63] Relatively minor alterations in pixels or the degree of noise in an image can lead an AI to conclude an image is a racecar when it is really a sloth. Cases where the data used to train an algorithm comes from an adversary could be particularly vulnerable to this problem.[64] In arms control, baseline information about capabilities is usually at least in part based on initial disclosure by the other party.

Even more advanced possibilities for exploiting AI in the context of national security issues are also becoming apparent. Research using GANs may allow a state to identify changes in the physical world that may be effective in duping an adversary's AI. States have always used decoys, but as reliance on AI grows, decoy tactics could become increasingly useful, as sometimes simple alterations can effectively fool an algorithm. Specifically designed stickers attached to a street sign, for example, can lead an AI to misidentify the sign as a completely different object.[65] Speaking at a DARPA colloquium in 2019, Hava Siegelmann used the sticker example to suggest how an adversary might attack AI-enabled detection tools by making a tank look like a delivery truck. Commenting more broadly on image detection, Seigelmann noted that "the feeling today in the field is that it is much easier to design [an] attack than to come up with defenses" and that DARPA is launching new research to study defenses against duping for various kinds of AI — including image classifiers, prediction, and decision-making — that can be generalized across different types of attacks.[66]

A state can also use AI to generate false information to conceal its military activities. Studies have shown progress in using AI to create "spoofed" images and videos.[67] By creating such fake content, AI could help states to obfuscate their real behaviors by making it "much easier to lie persuasively."[68] A GAN model can generate new images following

[60] Jason Pontin, "Greedy, Brittle, Opaque, and Shallow: The Downsides to Deep Learning," *Wired*, Feb. 2, 2018, https://www.wired.com/story/greedy-brittle-opaque-and-shallow-the-downsides-to-deep-learning/.

[61] Ian Goodfellow, et al., "Generative Adversarial Nets," in *Proceedings of Conference on Neural Information Processing Systems, Palais des Congrès de Montréal, Montréal, Canada, December 8–13*, https://papers.nips.cc/paper/2014/file/5ca3e9b122f61f8f06494c97b1afccf3-Paper.pdf.

[62] Jiajun Wu, et al., "Learning a Probabilistic Latent Space of Object Shapes via 3d Generative-Adversarial Modeling," in *Advances in Neural Information Processing Systems*, 2016, 82–90, http://3dgan.csail.mit.edu/.

[63] Nguyen, Yosinski, and Clune, "Deep Neural Networks Are Easily Fooled."

[64] Michael C. Horowitz "The Promise and Peril of Military Applications of Artificial Intelligence," *Bulletin of the Atomic Scientists,* April 23, 2018, https://thebulletin.org/2018/04/the-promise-and-peril-of-military-applications-of-artificial-intelligence/.

[65] Kevin Eykholt, et al., "Robust Physical-World Attacks on Deep Learning Visual Classification," *IEEE/CVF Conference on Computer Vision and Pattern Recognition*, (2018): 1625–34, https://doi.org/10.1109/CVPR.2018.00175.

[66] Hava Siegelmann,"Artificial Intelligence Colloquium: Lifelong and Robust Machine Learning," DARPAtv, video recording, March 26, 2019, https://www.youtube.com/watch?v=CmewHNgWQWY&t=846s. See in particular the section starting at 14:00.

[67] Amy Zegart, "The Tools of Espionage Are Going Mainstream," *The Atlantic,* Nov. 27, 2017, https://www.theatlantic.com/international/archive/2017/11/deception-russia-election-meddling-technology-national-security/546644/.

[68] Greg Allen and Taniel Chan, "Artificial Intelligence and National Security," Belfer Center for Science and International Affairs, Harvard Kennedy School, July 2017, https://www.belfercenter.org/publication/artificial-intelligence-and-national-security.

a certain style and set of attributes, as has been demonstrated publicly by websites that generate human faces, manipulate the facial features of movie stars, imitate styles of master painters, or colorize black and white photos.[69]

The ability to generate high-quality fake images also suggests that states could provide reporting data that intentionally undermine verification and intelligence-collecting efforts. Images of objects or buildings are easier to falsify than faces, and some of the cutting-edge biometric tools being developed to identify deepfakes, such as detecting a pulse in a video of a person,[70] clearly do not apply to objects. Recent research also suggests AI can be used for location spoofing and creating "deep fake geography."[71] Fake satellite images can mimic the landscape and physical features of real places while creating new structures, roads, or features.

The wide availability of commercial and national intelligence imagery mitigates some of the risks associated with a state supplying a spoofed image, but not all of them. Analysts can cross-check suspicious images by comparing them with other images from diversified sources. Even non-governmental experts are unlikely to be easily tricked. Nevertheless, spoofed imagery may allow a state that is attempting to hide a violation to sow doubt and create discord in the public debate, or to sway (even temporarily) the views of political decision-makers.[72] Further, if publicly debunking an image as manipulated would require revealing intelligence capabilities, it could put agreement monitoring in a particularly difficult position.

Using deepfake imagery could also allow an adversary to exploit a timing issue. An adversary could provide an image that will indeed be identified as manipulated, but that analysis process takes time, during which military or diplomatic decisions need to be made.[73] Particularly when it comes to arms control agreements that deal with more tactical or regional issues, such as deployments, tests, or military exercises, the difference of a few days may be sufficient for a concealed violation to matter.

Finally, agreement monitors have resource constraints. Intelligence agencies have to devote more and more resources to detecting spoofing as the sophistication of this technology increases. They also shoulder the burden of proof in countering information that seems real to the casual or even well-informed observer.[74] Todd Myers, an official at the National Geospatial-Intelligence Agency, noted at a 2019 conference that the intelligence community can detect GAN-generated images, but the process is time-consuming, costly, and requires the collection of extra images and corroborating evidence.[75] The presence of some fake images, even if they can be detected, could mean that many real ones need to be checked as well.[76]

In some agreements, verification can be informed by observing discrepancies or omissions in the material that another state provides about its activities. If reporting is found to be inaccurate, it can be an important indicator of underlying intentions, including an intention to secretly evade commitments. However, AI might be intentionally used to mislead and create advantages for the reporting state. A state's disclosures and self-reporting would be essentially tainted evidence, setting up baselines that make it difficult to identify real agreement violations. This information would be unreliable as a data source for training AI algorithms to detect future deviations. The prospect of sophisticated manipulation in reporting material decreases the usefulness of this type of information as a transparency tool and increases drain on resources to verify compliance. It may even increase security risks by allowing states to insert false intelligence information under the guise of standard treaty processes.

Overall, developments in AI seem likely to make agreements that do not include monitoring provisions easier to conclude due to the significant advantages that AI provides for unilateral monitoring.

[69] See for example, "Home Page," This Person Does Not Exist, accessed Sept. 14, 2021, thispersondoesnotexist.com; and "Home Page," DeOldify, accessed Sept. 14, 2021, https://deoldify.ai/.

[70] Patrick Tucker, "AI Will Make Fake News Video — and Fight It As Well," *Defense One*, Aug. 8, 2017, https://www.defenseone.com/technology/2017/08/ai-will-make-fake-news-video-and-fight-it-well/140075/.

[71] Bo Zhao et al., "Deep Fake Geography? When Geospatial Data Encounter Artificial Intelligence," *Cartography and Geographic Information Science* 48, no. 4 (2021): 338–52, https://doi.org/10.1080/15230406.2021.1910075.

[72] "Nuclear Monitoring and Verification in the Digital Age: Seven Recommendations for Improving the Process" Nuclear Verification Capabilities Independent Task Force of the Federation of American Scientists, Third Report, September 2017, https://fas.org/wp-content/uploads/media/Nuclear-Monitoring-and-Verification-in-the-Digital-Age.pdf.

[73] Author interview with Therese Jones, senior director of policy, Satellite Industry Association, April 30, 2021.

[74] Zegart and Morell, "Spies, Lies, and Algorithms."

[75] Patrick Tucker, "The Newest AI-Enabled Weapon: 'Deep-Faking' Photos of the Earth," *Defense One*, March 31, 2019, https://www.defenseone.com/technology/2019/03/next-phase-ai-deep-faking-whole-world-and-china-ahead/155944/.

[76] Zhao et al., "Deep Fake Geography?"

But, some caution is warranted, as AI applications may also introduce new uncertainty that is very difficult to measure. AI also provides few opportunities for demonstrable control, so efforts to apply AI-enabled tools in intrusive monitoring may undermine cooperation. Finally, in the future, AI may have the potential to aid in the concealment of both agreement violations and other capabilities. One might expect that being able to conceal capabilities that are not limited by an agreement would make agreements more likely by ameliorating the transparency-security trade-off. However, the scenarios discussed above suggest that the same methods would be even more effective for hiding violations and therefore diminish prospects for agreements.

Digital Additive Manufacturing

Additive manufacturing (AM), or "3D printing," may not be commonly thought of as a monitoring technology, but a closer look suggests a number of possible applications. Industrial-level AM uses materials (including plastics, metals, carbon and synthetic fibers, and many more) and a manufacturing device or "printer" to create items with physical properties matching or even outperforming equivalents produced through traditional subtractive manufacturing techniques. Digital build files contain design information for what will be printed, and additional software is used to "slice" files in preparation for printing.[77] AM is a "cyber-physical manufacturing technology that utilizes innovations in robotics, computation, and digital networks to enable the fabrication of physical components from digital build files."[78] In addition to commercial industry applications, states can use 3D printing to build specialized replacement parts for weapons and delivery systems. In the future, greater portions of the production line could rely on AM, though it is unlikely to replace traditional manufacturing. As they integrate AM into production activities both private and state actors will find more applications for the digital components of the process, which include files that contain build plans or data used for reliability testing. It is specifically this cyber-physical nature of 3D printing that has interesting implications for agreement monitoring and the transparency-security trade-off. For AM technology, it is useful to start with a discussion of how it could affect concealment, before turning to its effects on demonstrable control and unilateral monitoring.

In some ways, AM technology could be a boon for weapons proliferation. States could gain easier access to weapons components by printing them rather than importing or investing in industrial-level production. There are a number of contemporary military applications for 3D printing. There is already capability to print guns and other small arms, as well as sophisticated items such as components for missiles and aircraft engines.[79] The U.S. military and defense companies are actively researching AM applications for small, flexible weapons systems, munitions, and printed electronic components, such as health monitoring or communications components that are directly integrated into soldier's clothing. The U.S. Navy has pursued AM tools to replace parts for ships and submarines that traditional manufacturing no longer produces. The same 3D printing approaches are likely to be applicable for maintaining aging aircraft, such as the B-52 Stratofortress.[80] Looking forward, the services are considering scenarios where build files and polymers could be transferred to remote printers in order to provide replacement parts on demand.

At first glance, it appears likely that as 3D printing becomes increasingly integrated into military capabilities, enforcing arms control restrictions would become more difficult. Concealment of violations could be easier. The ability to build components more quickly, in flexible locations, and with very small manufacturing footprints will make monitoring and observation more challenging. This challenge could apply to imposing restraints on new capabilities, but it is even more illustrative to consider how AM would alter the ability to restrict older weapons.

Arms control treaties sometimes require states to decommission or otherwise disable certain armaments. States negotiate what will be considered sufficient disabling of a weapon, ensuring that the other side can verify the weapon's non-usability without collecting extra information about its design. However, with improvements in AM, previous-

[77] Marco Fey, *3-D Printing and International Security: Risks and Challenges of an Emerging Technology*, Peace Research Institute Frankfurt, Jan. 1, 2017, http://www.jstor.org/stable/resrep14453; and Grant Christopher, "3D Printing: A Challenge to Nuclear Export Controls," *Strategic Trade Review* 1, no. 1, (2015): 18–25, http://www.str.ulg.ac.be/wp-content/uploads/2016/01/2_3D_Printing_A_Challenge_to_Nuclear_Export_Controls.pdf.

[78] Wyatt Hoffman and Tristan A. Volpe, "Internet of Nuclear Things: Managing the Proliferation Risks of 3-D Printing Technology," *Bulletin of Atomic Scientists* 74, no. 2 (2018): 102–13, https://doi.org/10.1080/00963402.2018.1436811.

[79] Fey, *3-D Printing and International Security.*

[80] Amanda M. Schrand, "Additive Manufacturing: From Form to Function," *Strategic Studies Quarterly* 10, no. 3 (Fall 2016): 74–90, http://www.jstor.org/stable/26271495.

ly decommissioned weapons might be more easily reconstituted without creating observable signals, such as new manufacturing facilities or long repair processes. To address this problem, agreements would need more intrusive and longer-lasting monitoring to be viable, which in turn would increase the security risks for monitored states. If 3D printing creates a need for greater intrusiveness to verify that old weapons stay out of commission, it would exacerbate the transparency-security tradeoff and make agreements less likely.

However, 3D printing could make arms control agreements easier to conclude by providing new transparency options and a potentially high degree of demonstrable control over what information is revealed for compliance purposes. It is possible to imagine a scenario in which AM is not being used as a monitoring tool itself, the way a satellite or camera might be, but rather in which a state's use of AM to manufacture a weapons capability provides options for information gathering and reporting. From this perspective, there are two possible pathways for transparency and demonstrable control. First, the AM process is more digital in nature than traditional manufacturing, which allows for completely different ways of observing and tracking manufacturing processes. 3D printers rely on digital build files for instructions on what to do and the printing process itself is controlled by a computer. Components can also be networked. Different inputs are going into the process, including highly specialized materials, and more data is generated about what is occurring in the manufacturing process over a shorter time frame. In this context, AM is also a monitoring technology.

Actors that use 3D printing could give external observers access to the digital files they use for production to demonstrate that banned components are not being built. In a traditional manufacturing context, observers might be concerned that human expertise or equipment will be diverted to building other military capabilities. The employment of digital build files in AM technology means that a state would not need extensive knowhow or advanced manufacturing equipment to reach certain capabilities.[81] It could therefore be easier for a monitoring side to get assurance that the monitored state is only building approved components and not using the technology to build other restricted capabilities. In the cases where suppliers seek to impose export control, higher reliance on AM with safeguarded build files could allow for easier verification by narrowing the need to collect additional information to detect the prohibited use of manufacturing tools. Digital management of the supply chain could also create an easier way for a state to demonstrate that it is adhering to the quantitative or qualitative limits on the production of a particular capability. Suppliers exporting controlled capabilities can also provide build files that cannot be easily altered to use 3D printing for non-approved purposes.[82]

3D printers are "Internet of Things" machines that use embedded sensors at various points in the process.[83] There are commercial advantages to setting up sensors for data collection. A manufacturer can do quality-control checks and conduct any necessary certifications, such as evaluating the reliability of the material, during the build process itself. This can improve efficiency by eliminating a step later in production and allowing manufacturers to make course corrections early on if a problem is detected.[84] This digital process may also allow monitored states to credibly reveal that they are in compliance with an agreement. When an AM process is being used, it gives a state the ability to reveal specific process steps and information points. Suppliers or monitoring parties likewise would have the ability to demand fine-grained, narrow information relevant to compliance. This allows for a high degree of control of what information is revealed to sufficiently prove compliance, as well as a way to make that control demonstrable by allowing access to digital data collection.

While the digital nature of 3D printing can increase transparency, it might also create new threats to security. Use of AM may provide a new avenue for espionage by creating access that is less voluntary than the data-sharing ideas discussed above. Networked systems increase the risk of cyber intrusions for both intelligence gathering and malicious modifications or destruction during the manufacturing pro-

[81] Tristan A. Volpe, "Dual-Use Distinguishability: How 3D-Printing Shapes the Security Dilemma for Nuclear Programs," *Journal of Strategic Studies* 42, no. 6 (2019): 814–40, https://doi.org/10.1080/01402390.2019.1627210.

[82] These points, and several examples in the following paragraph, draw on Hoffman and Volpe, "Internet of Nuclear Things."

[83] Md Masud Rana and Narendra Dahotre, "IoT-Based Cyber-Physical Additive Manufacturing Systems: A Secure Communication Architecture, Research Challenges and Directions," 6th International Conference on Inventive Computation Technologies (ICICT), 2021, https://doi.org/10.1109/ICICT50816.2021.9358643.

[84] DE Editors, "Editor's Pick: Real-time Process Monitoring for Metal Additive Manufacturing," *Digital Engineering*, no. 247, May 22, 2019, https://www.digitalengineering247.com/article/real-time-process-monitoring-for-metal-additive-manufacturing/simulate; and Chris Hole, "Cost and Practicality of In-Process Monitoring for Metal Additive Manufacturing" *Metal AM* 2, no. 4 (Winter 2016), https://www.metal-am.com/articles/cost-and-practicality-of-in-process-monitoring-for-metal-3d-printing/.

cess. The effect on arms control is mixed. For states seeking to detect agreement non-compliance, such cyber vulnerabilities in the monitored state could increase their confidence in unilateral monitoring and make them more willing to accept a deal without additional inspections. But because cyber access often blurs the line between espionage and manipulation, monitored states may fear that efforts to detect violations will incentivize attacks, and so be unwilling to negotiate over any capabilities produced through vulnerable 3D printing.

Second, despite the high degree of control over information that AM would provide in a cooperative monitoring context, the transparency-security tradeoff does not fully disappear. States relying on digital 3D printing may still fear that voluntary information sharing about those processes could reveal significant intelligence. For example, by knowing what kind of replacement parts a state is producing, an adversary could make deductions about the reliability or readiness of the state's military capabilities. It may reveal that some capability is likely to have a higher failure rate or may be going out of service in the near future. The extent of the security risk is likely to depend on how widely AM is being used. If AM is used in numerous military applications, information about one area of production could reveal details about others. But, if AM use is relatively isolated, then information about other capabilities would be less at risk.

To assess the overall effects of this technology on arms control, it is useful to consider scenarios in which states use AM as opposed to traditional manufacturing for a weapons capability, or perhaps even in which an agreement mandates AM as the agreed upon process for future production. In some ways, 3D printing provides states with a higher potential to conceal violations. But, it also provides unique opportunities for transparency that may mitigate those concealment risks. Innovation in cyber security for AM components may reduce the ability to unilaterally monitor systems, but it is likely to be a net benefit for cooperation if it allows states to rely on digital transparency for demonstrable control in mutually accepted monitoring regimes.

Conclusion

In contemporary policy discourse, there is sometimes a sense that arms control means benevolent cooperation with another state. In reality, however, arms control is just as close to being a coercive tool as it is a cooperative one. Steps taken in an agreement serve the interests of each side, and indeed each side will try to get the more favorable distribution of benefits, or more advantageous information, in the process of negotiating and enforcing an agreement. In this light, the security risks of agreement monitoring are less surprising. Arms control negotiators regularly face concerns over espionage and security vulnerabilities as part of any agreement monitoring plan. The use of agreement verification for intelligence collection is accepted as a reality, even if it is not frequently talked about in the portrayals of monitoring as mutually beneficial for assuring compliance.

Technological change has the potential to significantly alter how states parties to an agreement get compliance information. But while some changes will make it easier for states to sign agreements, others are likely to increase security risks and diminish incentives for formal cooperation. As the analysis of specific technologies presented in this article has shown, the same set of technological changes can have countervailing effects on the prospects for cooperation — on the one hand, providing greater assurance that cheating will be detected, and on the other hand, creating greater concern that secrets will be revealed.

This article has argued that specific characteristics of an emerging technology matter when it comes to thinking about how it will affect monitoring, the transparency-security trade-off, and ultimately the prospects for an agreement. An assessment focused on unilateral monitoring, demonstrable control, and concealment will provide the clearest predictions for whether greater integration of a particular technology into agreement monitoring, as well as into sensing and intelligence capabilities in general, will make arms control agreements easier to negotiate. Future research should seek finer-grained evaluation and measurement of these factors. After all, if countervailing forces exist, we ultimately want to know which direction will be stronger and whether cooperation may still be possible.

More broadly, emerging technology will likely have effects on arms control agreements through pathways other than changes in monitoring. For example, technologies such as hypersonic and anti-satellite weapons may have effects on strategic stability.[85] This could, in turn, affect the arms control calculus, perhaps increasing incentives for cooperation in scenarios where emerging capabilities are useful for some missions but also destabilizing. A wider version of the core question addressed in this article would need to tackle how innovation in military technology in general, beyond monitoring

[85] Chyba, "New Technologies and Strategic Stability."

applications, may have implications for efforts to use bargains to limit capabilities and risks.

The assessment presented here is far from exhaustive, even with regard to the types of technologies discussed, but it does provide a tool for assessing other types of technology. Some technologies not addressed in this article could expand monitoring capabilities in ways that increase transparency while protecting security. For example, distributed ledger, or "blockchain," technology is used commercially to document information transfers, improve logistics, and track inventory. Future private-sector applications could include monitoring supply chains and improving supply chain security.[86] Perhaps similar tracking methods could be used to improve military export control regimes, mitigating the likelihood of items being misdirected to alternative users without requiring supplier states to reveal more details about military or commercial applications of specific transfers. The framework presented in this paper gives scholars and practitioners a starting point for both assessing other technologies and revising past assessments in response to further innovations and practical experience.

Analysis of the cases presented in this article suggests that there is reason for pessimism about new, more effective ways to detect arms control noncompliance, particularly when it comes to cooperative (rather than unilateral) monitoring. The benefits of verifiable cooperation may simply be outweighed by fears of security breaches, either real or perceived. Uncertainty about the capabilities of monitoring tools, which is likely to be heightened with today's emerging technologies, further exacerbates the security threat side of the trade-off. At the same time, reducing uncertainty by sharing technical details with an arms control partner is complicated by the general-purpose nature of most of the capabilities being considered. For example, AI algorithms used to analyze treaty-related images may also have other military applications, in which case revealing the algorithm details would degrade those capabilities. In the end, it may be that traditional monitoring and verification tools, such as cameras and human eyes, remain the mainstay of arms control treaty design, not because they are so good at detecting violations but rather because the intelligence-gathering potential of these methods is well understood and calculable for prospective arms control scenarios.

Despite the words of caution, this analysis also motivates three concrete recommendations for policy interventions. First, policymakers and independent experts should seek to refocus the question of arms control "verifiability" on publicly accessible, non-intrusive tools, such as satellites and other forms of remote sensing. There has long been a strong push in the United States for on-site inspections as part of many types of arms control deals. Some actors may seek inspections for domestic political reasons or even explicitly to improve espionage collection. The "best practices" culture within the arms control community also favors inspections and transparency. However, these requirements may undermine deals due to the risks they introduce for the inspected state and for the inspecting state as well, when inspections are reciprocal. Framing verifiability requirements in the context of publicly accessible information, perhaps even using a term like "international technical means," can leverage the growing advances in remote sensing in government and private sectors, and also create benefits by relying on information collection methods that are not themselves sensitive.

Second, the use of emerging technology in intrusive inspections will be difficult, but it does have exciting promise and should be explored. Addressing the transparency-security trade-off will be critical in any implementation attempt. One way to do this will be through improving capabilities for demonstrable control. A key path forward may be through "co-development" of applications and tools alongside experts in other countries. There may be no way to convince another country that a U.S.-built AI tool is limited in a particular way, and the United States would be unlikely to believe such claims from an adversary. But, by engaging in joint development of a specialized AI application, undertaken together from the ground up, the mutual understanding of its capacity and limits might be much greater. Such technical cooperation is not a new idea: The United States and the Soviet Union did it during the Cold War even during moments of tense relations.[87] In light of the opportunities and uncertainties of today's emerging technologies, there is a renewed imperative for these kinds of collaborations.

Finally, policymakers should encourage new research on how emerging technology can help states that are in compliance with an agreement to demonstrate their good behavior in cost-effective, credible, and secure ways. The agreement monitor-

[86] Robin Lineberger, et al., "Aerospace and Defense 4.0: Capturing the Value of Industry 4.0 Technologies," Deloitte Insights, 2019, https://www2.deloitte.com/insights/us/en/focus/industry-4-0/aerospace-defense-companies-digital-transformation.html; and Eric Piscini, Gys Hyman, and Wendy Henry, "Blockchain: Trust Economy," in *Exponential Manufacturing: A Collection of Perspectives Exploring the Frontiers of Manufacturing and Technology* (Westlake, TX: Deloitte University Press, 2017).

[87] "Home Page," Doomed to Cooperate: US-Russian Lab-to-Lab Collaboration Story, accessed August 2021, https://lab2lab.stanford.edu/.

ing conversation usually takes place from the point of view of one side seeking to detect noncompliance while the other side seeks to hide violations or hide non-treaty limited capabilities. But considering the perspective of states which intend to comply with agreement terms may provide alternative avenues for establishing new governance approaches in international security. While the mechanism of self-reporting has long been a part of international law, both in security agreements and more broadly in areas of human rights, environment, and trade,[88] this has traditionally been treated as a weak tool for ensuring compliance. However, perhaps technology developments can allow states to choose to reveal information that verifiably proves compliance while allowing them to protect information that increases security risk. Some similarly minded applications have already emerged in the environmental security space. For example, with regard to fisheries, producers can use data on ship geolocations and AI-enabled tracking of fish types and amounts to prove to regulators and consumers that they are complying with sustainability standards.[89] If a sensing, analytic, or tracking technology can help improve self-reporting in arms control, then states genuinely seeking to reap the benefits of mutual restraint would be more likely to sign on to formal agreements, while the hesitation of other states to do so may itself be telling.

Emerging technology will undoubtedly continue to affect multiple aspects of international security, in ways both anticipated and unanticipated. Scholars and practitioners should continue to develop analytic tools to evaluate and compare the implications of those effects. The intersections between technology and security cooperation, both specifically in the arms control context discussed here, but also in other areas such as alliances, transnational threats, and international institutions, warrant closer attention, particularly because the consequences of technological change are likely to be complex and not universally beneficial. A multifaceted analytic lens will be important in informing specific contexts, like treaty negotiations, in which policymakers will need to make choices about how to address technological developments, whether as tools for improving regime effectiveness, as obstacles in negotiations, or as drivers of new approaches to cooperation. ♝

Dr. Jane Vaynman *is assistant professor of political science at Temple University.*

Acknowledgements*: I would like to thank Francis Gavin, Kori Schake, James Steinberg, Keren Yarhi-Milo, and Amy Zegart for comments on this article. Earlier versions of this paper were presented at POSSE Workshop on Emerging Technologies and Strategic Stability (Washington D.C., 2018) and the NSRI & IFSH conference "Rethinking the Nuclear Future: Perspectives from Europe and America," (Hamburg, Germany, 2019). I thank the participants for their comments.*

Image: Marcho Verch (https://www.flickr.com/photos/30478819@N08/48899819763/in/photostream/); CC BY 2.0 (https://creativecommons.org/licenses/by/2.0/)

[88] Cosette D. Creamer and Beth A. Simmons, "The Proof Is in the Process: Self-Reporting Under International Human Rights Treaties," *American Journal of International Law* 114, no. 1 (January 2020): 1–50, https://doi.org/10.1017/ajil.2019.70.

[89] Melina Kourantidou, "Artificial Intelligence Makes Fishing More Sustainable by Tracking Illegal Activity," *Phys.org*, July 12, 2019, https://phys.org/news/2019-07-artificial-intelligence-fishing-sustainable-tracking.html; and Meg Wilcox, "The Future of Fishing Is Big Data and Artificial Intelligence," *Civil Eats*, May 10, 2018, https://civileats.com/2018/05/10/the-future-of-fish-is-big-data-and-artificial-intelligence/.