JANUARY 2022

Integrated Arms Control in an Era of Strategic Competition

AUTHORS
Rebecca K.C. Hersman
Heather Williams
Suzanne Claeys

A Report of the CSIS Project on Nuclear Issues

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

JANUARY 2022

Integrated Arms Control in an Era of Strategic Competition

AUTHORS
Rebecca K.C. Hersman
Heather Williams
Suzanne Claeys

A Report of the CSIS Project on Nuclear Issues

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

ROWMAN & LITTLEFIELD

Lanham • Boulder • New York • London

About CSIS

The Center for Strategic and International Studies (CSIS) is a bipartisan, nonprofit policy research organization dedicated to advancing practical ideas to address the world's greatest challenges.

Thomas J. Pritzker was named chairman of the CSIS Board of Trustees in 2015, succeeding former U.S. senator Sam Nunn (D-GA). Founded in 1962, CSIS is led by John J. Hamre, who has served as president and chief executive officer since 2000.

CSIS's purpose is to define the future of national security. We are guided by a distinct set of values—nonpartisanship, independent thought, innovative thinking, cross-disciplinary scholarship, integrity and professionalism, and talent development. CSIS's values work in concert toward the goal of making real-world impact.

CSIS scholars bring their policy expertise, judgment, and robust networks to their research, analysis, and recommendations. We organize conferences, publish, lecture, and make media appearances that aim to increase the knowledge, awareness, and salience of policy issues with relevant stakeholders and the interested public.

CSIS has impact when our research helps to inform the decisionmaking of key policymakers and the thinking of key influencers. We work toward a vision of a safer and more prosperous world.

CSIS does not take specific policy positions; accordingly, all views expressed herein should be understood to be solely those of the author(s).

ISBN: 978-1-5381-4051-2 (pb); 978-1-5381-4052-9 (eBook)

Center for Strategic & International Studies
1616 Rhode Island Avenue, NW
Washington, DC 20036
202-887-0200 | www.csis.org

Rowman & Littlefield
4501 Forbes Boulevard
Lanham, MD 20706
301-459-3366 | www.rowman.com

Acknowledgments

The authors would like to thank all of the workshop participants who offered valuable insights and sparked thoughtful discussions. The authors would also like to thank David C. Logan, Dr. Justin Anderson, and Elaine Bunn, who reviewed earlier drafts of the report and provided valuable feedback. The authors would also like to thank Eric Brewer for his close readings and recommendations for later versions of the report. Finally, the authors appreciate the support of CSIS's iLab team in the editing, formatting, and publishing of the report.

This research was made possible through the support of the United States Office of the Deputy Assistant Secretary of Defense Threat Reduction and Arms Control (ODASD(TRAC)). The opinions, findings, views, conclusions, or recommendations contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of ODASD(TRAC) or the U.S. government.

Contents

Executive Summary

Can contemporary arms control keep pace with the rapid rate of change in both geopolitics and technology? The increasingly competitive security environment has made near-term prospects for further reductions in nuclear arms and delivery systems unlikely, yet fundamental interests in strategic stability, risk reduction, and the prevention of arms racing remain. Indeed, the challenges to future arms control—the decline in trust between the United States and potential arms control partners; the rise in complex, highly interrelated, strategic technologies; the emergence of a highly digitized, privately controlled, and easily weaponized information environment; and the presence of increasingly assertive regional stakeholders—all point to a rocky road ahead. Measures that build confidence, reduce miscalculation, enhance transparency, and restrain costly and dangerous military competition may be of increasing value, particularly as states develop and employ a wider range of strategic technologies and rely on broader strategic concepts such as integrated deterrence to reduce the risk of conflict between major nuclear-armed powers. Moreover, arms control institutions and mechanisms for dispute resolution and compliance enforcement can provide useful venues for addressing sources of conflict, reducing misperceptions, and restraining impulsive or risky actions.

For arms control tools to succeed, however, they must be adapted to the current security environment, account for rapidly evolving technological and informational factors, and consider alternative structures, modalities, and participation models. As deterrence becomes more integrated across an increasingly diverse range of technologies, domains, risks, and actors, so too must arms control. Indeed, now is the time for a recoupling of arms control with deterrence in a way that recognizes these new realities. Now is the time for integrated arms control.

The Evolving Technology Landscape

For most emerging and potentially disruptive technologies, private actors, rather than governments, are the primary developers and drivers of innovation. Also, the rapid way in which these technologies are being developed, fielded, and updated is straining the ability of existing legal mechanisms and arms control institutions—often more rigid and slower to adapt—to keep up. Finally, many of these technologies are still under development, and both states and private companies might be unwilling to subject them to limits that could curtail future economic or military advantage. This evolving technological landscape has three broad implications for arms control: (1) emerging technologies complicate strategic stability and risks of crisis escalation and arms racing; (2) many of these advanced technologies are used in both the civilian and military sectors, complicating the ways in which arms control agreements are negotiated and implemented, and (3) most of these technologies exist outside of existing arms control regulations, meaning legal mechanisms will likely struggle to incorporate them.

The Evolving Information Ecosystem

Today's information ecosystem, specifically the potential benefits and challenges for accessing, processing, analyzing, altering, and disseminating large volumes of information, is poised to change the nature of arms control.[1] This complex and highly dynamic information environment will potentially transform how agreements are negotiated, monitored, verified, and enforced, not to mention altering roles and responsibilities along the way. First, the use of disinformation to undermine arms control structures, institutions, and mechanisms poses a large and growing challenge to future arms control. Manipulated information could be used to raise questions about a country's compliance with an arms control agreement, forge or fake a treaty violation, cover up or hide a violation, or cause confusion about a state's weapon development. Second, state actors are not the only players of note in the new information ecosystem. The explosion of international open-source investigation and analysis groups outside the government will potentially transform not only how verification is done but also who does it. In the future, open-source information may offer monitoring and verification alternatives when intrusive, state-sponsored approaches might not be agreeable or desirable. Ultimately, this emerging information ecosystem, particularly in the form of highly competitive open-source analysis and investigation, will impact the role of national technical means (NTM)—nationally controlled ground, space, airborne, or even underwater sensors—in monitoring and verifying compliance with arms control agreements.[2]

Evolving Concepts of Escalation and Stability

Cold War stability concepts drew heavily on ladders and firebreaks to define nuclear crises and escalation, but contemporary deterrence failure may more closely resemble "wormholes" or sudden, possibly temporary openings in the fabric of deterrence that allow for accelerated and unpredictable escalation risks. Future conflicts are unlikely to unfold in a clear linear or stepwise fashion with a distinction between pre-conflict and conflict termination. Neither is a clear delineation between nuclear and non-nuclear crises sustainable when conventional and nuclear capabilities are highly co-mingled, capable of more diversified strategic effects, and increasingly vulnerable to detection, disruption, or disablement.[3]

Integrated deterrence strategies can only provide partial answers to this complex and multidimensional strategic challenge. In fact, in a deterrence framework that is much larger and more comprehensive than traditional nuclear deterrence, gaps and weaknesses that create the potential for wormhole dynamics are more likely, not less. Moreover, the very nature of integrated deterrence erodes the utility of firebreaks in arresting stability risks as capabilities grow more entangled. In a security paradigm based on integrated deterrence, the imperative for arms control is more urgent than ever. By identifying and mitigating deterrence gaps and risks, future arms control may prove most useful by focusing on preventing conflict as well as costly arms races that might incentivize nuclear first use or crises that can rapidly escalate. Rather than seeking to impose numerical constraints on specific technologies, states might prioritize arms control efforts that target specific behaviors of concern, regardless of the technological capabilities involved, and explore a wide range of arms control modalities to reduce the risks of arms racing and improve crisis stability.

Conclusions and Recommendations: Realizing an Integrated Arms Control Strategy

This highly entangled, multidomain risk landscape suggests new approaches to strategic arms control will be needed to mitigate risks across both technical domains and levels of conflict. In addition, the status of China as a rising peer, accompanied by increasingly capable regional nuclear actors, suggests multi-actor and multifocal approaches will need to replace traditional bilateral ones. Going forward, while the broader goals of disarmament may be desirable, the most pressing objective for arms control in the current security environment must be the prevention of major war, especially war that would occur under a dangerous nuclear shadow, which risks catastrophic escalation in the event of deterrence failure. It is in identifying and mitigating such deterrence gaps and risks, as well as the costly arms races that may well accompany them, that future arms control—integrated arms control—may prove most useful.

Integrated arms control should be based on three broad principles: enhancing stability, embracing plurality, and reinforcing resiliency. First, arms control remains a tool for strategic stability and managing risks associated with crisis escalation and arms racing. This can, and should, work hand in hand with deterrence, and integrated arms control should be part of any integrated deterrence strategy. Second, arms control will need to be flexible and operate across a plurality of technologies and actors. Integrated arms control must be multidomain, multilateral, and agile. Amid geopolitical and technological changes, strategic stability is becoming increasingly complex and will require a more flexible approach to arms control than is typically provided by legally binding bilateral agreements that focus on single technologies or domains. Finally, an effective integrated arms control strategy will require that the United States organize and invest to create the structural, technical, and operational capabilities necessary to support such an approach in ways that are durable and sustainable.

ENHANCING STABILITY

- **Recognize arms control as a constructive forum and outlet for strategic competition.** Nuclear arsenals that are expanding both quantitatively and qualitatively, accompanied by a broader set of strategic delivery systems and high-impact technologies, which will challenge existing U.S. defensive systems. Meanwhile gray zone activities will further complicate concepts of escalation. Arms control can offer the United States, China, and Russia

an opportunity to compete openly and fairly in a diplomatic forum that reduces risk and encourages stability.

- **Prioritize efforts that mitigate escalatory pressures that raise the risk of major war between nuclear-armed states**. While broader goals of disarmament may be desirable, the most pressing objectives for arms control in the current security environment must be preventing major war and reducing the risk of catastrophic escalation in the event of deterrence failure.
- **Address a range of stability challenges across multiple domains and technology types.** Nuclear arms control, such as a follow-on agreement to New START, remains critically important. However, it should not be prioritized to the exclusion of other arms control and risk reduction efforts in other arenas, such as biotechnology, advanced missile threats, space, cyber, and digital technologies, in which stability risks, both in terms of crisis management and arms racing, are of growing concern.
- **Focus on particularly risky behaviors, especially the application of advanced technologies during crisis scenarios.** Arms control arrangements that focus on banning or limiting specific numbers and types of weapons will continue to play a role in strategic stability, especially in terms of nuclear weapons and related delivery systems. But the intersection of nuclear and advanced technologies, especially during crises with compressed decisionmaking time, will also need to be a priority. Such agreements could address behaviors across the range of conflict that might erode or destabilize an integrated deterrence framework. Some specific priority areas for integrated arms control and risk reduction efforts that might address these behaviors include:

  Decision Interference: Actions that deprive leaders of the ability to communicate with their citizenry and control military forces suggest that arms control approaches should focus on fail-safe decisionmaking, such as reciprocal agreements to prohibit digital identity manipulation of national decisionmakers and others within the nuclear chain of command, or establishment of cyber or space-based "no go" zones designed to support risk reduction by protecting command, control, and communications.

  Predictive Surveillance: Arms control and confidence-building measures focused on protected opacity, shared warning data, strategic military deconfliction mechanisms, and notification requirements may help to ameliorate the downside risks associated with dramatic improvements in strategic warning systems.

  Autonomous Strike: Operator-in-the-loop requirements as well as AI-enabled "fail-safe" capabilities that improve nuclear weapons security, ensure continuous positive control, and better detect warning errors will be needed as accelerated and autonomous strategic strike systems are developed.

  Conventional Firebreaks: Faced with eroding strategic-level firebreaks, integrated deterrence approaches that prioritize preventing major warfare between major nuclear armed powers will require renewed focus on conventional arms control that seeks to contain and manage crises at lower-focus echelons of conflict, including curtailing risky behaviors in space, declared surveillance activities, separation of forces and assets agreements, limits on military exercises in border regions, and established payload limitations on high-maneuverability, intermediate, and long-distance strike platforms.

EMBRACING PLURALITY

- **Expand cross-domain, non-like-for-like approaches in future agreements.** With advanced technologies and cross-domain challenges, strategic stability may be better reinforced through arms control efforts that utilize cross-domain, mixed technology trade space. This concept of asymmetric arms control can facilitate more creative ideas for agreements across actors and domains.[4] Such agreements might include the exchange of non-like-for-like capabilities, or it might entail a broad overarching agreement that allows states to structure their forces asymmetrically within the terms of the agreement.
- **Incorporate new technologies, such as gene editing or offensive cyberattacks, into existing agreements, specifically in military contexts.** For example, military applications of CRISPR DNA and other forms of genome editing might be addressed through the Biological Weapons Convention.
- **Prioritize allies, partners, and other essential stakeholders' perspectives in pursuing integrated arms control.** Going forward, allies and partners' perspectives and inputs will be crucial to develop arms control agreements that address the diversity of issues involved and the asymmetry of stakes among various participants. In some instances, allies and partners might be amenable to being more formally involved in existing agreements, particularly those focused on risk reduction, as occurred in the Creating an Environment for Nuclear Disarmament (CEND) initiative. More ambitious involvement might include participation in consultative and ad hoc advisory bodies or affiliation with existing and new mechanisms, especially those that improve resiliency and address regional security concerns. Ultimately, however, this will depend on allies and partners' priorities and interests, in consultation with the United States.
- **Support stronger capacity-building efforts among allies and partners to improve technical capacities for arms control.** That will include verification, monitoring, investigations, forensics, and attribution efforts as well as sharing expertise and technical knowledge in these areas. Cooperative threat-reduction programs at the Departments of Defense and State bring considerable expertise and experience in these areas that could be adapted to the needs of an integrated arms control strategy.
- **Create positive incentives for multilateral cooperation in risk reduction efforts.** In areas of dual-use technologies, arms control partners can focus on agreements that offer more "carrots" rather than "sticks," such as access to shared technology, preferred trade and market access, and technical capacity building, especially in areas such as threat detection, investigations, forensics, and emergency response. Risk reduction efforts could be particularly valuable in promoting safe science initiatives to regulate dramatic advances in technology, such as codes of conduct among scientific communities to preserve benefits while mitigating security risks and to enhance multilateral oversight of dual-use research of concern.
- **Catalogue existing risk reduction and stability promoting tools through multilateral forums, such as the P5 process.** Integrated arms control will not necessarily require inventing new structures or tools. Indeed, numerous mechanisms already exist to promote strategic stability, particularly crisis stability, such as hotline agreements. Many of these, however, are underutilized or less well known. As part of their work on strategic risk reduction, the P5 process or the CEND initiative, in partnership with nongovernmental experts, should catalogue existing mechanisms for risk reduction. This could include efforts such as identifying and disclosing existing hotline

mechanisms, encouraging sharing of such mechanisms across the P5, broadening membership and reach of the Nuclear Risk Reduction Center network, and pursuing multilateral crisis communications, such as through CATALINK, a collaborative "hotline" project led by the Institute for Security and Technology.[5]

REINFORCING RESILIENCY

- **Emphasize dispute resolution mechanisms.** These can include expanding compliance reporting pathways and investigatory procedures, cooperative consultative processes, and implementation review bodies. These mechanisms might accompany robust verification activities, such as on-site inspections, or could be part of more informal agreements that might not have intrusive monitoring or verification beyond NTM. Indeed, as artificial intelligence (AI), open-source analysis, and other digital verification tools become more advanced, the amount of enforcement and compliance data that will require clarification and forums for dialogue could grow significantly.
- **Increase investment in research and development of arms control technologies designed to improve remote monitoring, enhance technical verification, better detect violations, and improve confidence in technical compliance while reducing intrusive requirements.** The Defense Threat Reduction Agency and the national laboratories are well equipped to focus on the technical requirements of integrated arms control and to create the implementation technologies necessary to be effective and enforceable.
- **Expand the cadre of qualified U.S. operational, technical, and policy personnel capable of supporting integrated arms control efforts.** Integrated deterrence as a military strategy will be implemented through a vast network of military planners, operators, and resource managers at the military services and combatant commands as well as policy professionals and the Joint Staff. Comparatively, the interagency human capital devoted to integrated arms control is vastly under-resourced at a time when arms control "multitasking" will be needed to engage across a diverse set of security imperatives.
- **Formalize and professionalize the role and development of open-source monitoring and verification in arms control agreements and institutions.** The United States should encourage collaborative efforts through private entities and international institutions to create codes of conduct, peer review processes, and standards of evidence for open-source analysis. This will especially require supporting the development and professionalization of open-source verification, monitoring, and analysis, while simultaneously maintaining clear separations from proprietary government sources of information such as intelligence and NTM.
- **Establish information security as a fundamental component of arms control, from negotiation to implementation.** Comprehensive, end-to-end information security practices to combat disinformation and influence operations should be built into all stages of the arms control process. Future agreements will be negotiated and implemented in a complex, technology-driven, and easily weaponized digital information ecosystem. Information security practices will be essential to counter the influence operations and other digital information risks that will be a feature of future arms control from negotiation to implementation and compliance.

Introduction

Can contemporary arms control keep pace with the rapid rate of change in both geopolitics and technology? For many observers, the gloomy prospects for arms control are exacerbated by an increasingly competitive and contested security environment and the decline in trust between the United States and arms control partners and stakeholders. And yet, while the continued numerical reductions of nuclear arms and delivery systems that characterized previous arms control agreements may prove elusive, fundamental interests in strategic stability, risk reduction, and the prevention of arms racing will remain. Indeed, in a more competitive security environment characterized by high risks and limited resources, there may be increasing value in measures that build confidence, reduce miscalculation, enhance transparency, and restrain costly and dangerous military competition. Moreover, arms control institutions and mechanisms for dispute resolution and compliance enforcement can provide useful venues for addressing sources of conflict, reducing misperceptions, and restraining impulsive or risky actions.

In fact, the importance of arms control as a tool for managing competition will only grow as states develop and employ a wider range of strategic technologies and rely on broader strategic concepts such as integrated deterrence to reduce the risk of conflict between major nuclear-armed powers. For arms control tools to succeed, however, they must be adapted to the current security environment. This means they must account for rapidly evolving technological and informational factors and consider alternative structures, modalities, and participation models. As deterrence becomes more integrated across an increasingly diverse range of technologies, domains, risks, and actors, so too must arms control. Complexity in strategic stability can, and should, be reflected in arms control. This range of issues will inform underlying dynamics that will shape future arms control priorities, negotiations, and implementation. Failure to adapt and change such approaches to the new reality may further undermine the prospects and utility of such agreements, both current and future.

Arms control institutions and mechanisms for dispute resolution and compliance enforcement can provide useful venues for addressing sources of conflict, reducing misperceptions, and restraining impulsive or risky actions.

This study examines the implications and prospects for the future of arms control in a highly competitive security environment in which challenges from advanced technologies and diminished state control over processes of verification become increasingly prominent features, even as the scope and modalities of arms control grow more complex and multifaceted. Specifically, the study examines three central questions:

- How is the current highly competitive security environment reshaping both opportunities and challenges for arms control in the years ahead?
- How can arms control be adapted to improve crisis management, reduce arms racing, and support strategic stability in light of today's security challenges?
- How might strategies of integrated deterrence inform arms control approaches and requirements? How can arms control account for the range of domains, technologies, risks, and actors that will shape approaches to integrated deterrence?

The report incorporates two years of discussions and insights by workshop participants from U.S. and European universities, think tanks, and various research organizations. While integrated deterrence emerged as a theme in the later stages of the project, it nonetheless provides a useful concept for considering the future of arms control. The result of these efforts is essentially a landscape analysis—a reexamination of the broad contours of arms control and its role in managing competitive security risks and challenges and the implications for U.S. policymakers, academics, and strategic thinkers engaged in U.S. nuclear policy. This landscape analysis concludes that arms control might be harder to achieve today due to a series of factors and trends in the international security environment, including:

- The decline in trust between the United States and potential arms control partners;
- The rise in complex, highly interrelated strategic technologies;
- The emergence of a highly digitized, privately controlled, and easily weaponized information environment; and
- The presence of increasingly assertive regional stakeholders.

Despite these challenges, both the need and the opportunity for arms control remain. In fact, the intersection of high risks, increasingly disruptive technologies, and limited resources that define the current security environment may also create an arms control "moment." Such a moment calls for a recoupling of arms control with deterrence in a way that acknowledges the integrated, cross-domain nature of the threats and the tools to address them. This is a moment for integrated arms control.

The first section of this report describes the evolving security environment and the ways in which strategic competition and integrated deterrence will drive both the need and the opportunity for arms

control. The second section discusses the primary drivers for strategic arms control integration: the emergence of an increasingly dual-use, highly interconnected military technology landscape with a broader array of strategically significant capabilities; the evolving information ecosystem and its implications for how future agreements can be negotiated, implemented, and enforced; and emerging concepts of escalation and strategic stability and their attendant implications for arms control and risk reduction. The third section of the report fleshes out the evolving modalities, structures, and tools available for arms control and offers a menu of options for future agreements. Finally, the report's key findings and recommendations focus on medium-term efforts for the U.S. policy community and note the vital and complementary role arms control can play in supporting a more stable and sustainable framework for integrated deterrence. The appendix includes brief case studies looking at chemical weapons use and Covid-19 to offer insights into how the information ecosystem may shape arms control in the future.

1

The Evolving Security Environment

Integrated Deterrence and Strategic Competition

Arms control and strategic competition are not mutually exclusive. Indeed, classic thinking on arms control, such as that offered by Thomas Schelling, emphasized that arms control and deterrence can work in tandem to manage competition and its associated risks, but that does not necessarily equate to either disarmament or a weakening of deterrence and strategic obligations. As the strategic landscape and deterrence requirements change, so must arms control. With that in mind, it is important to begin this analysis of arms control with a discussion of deterrence and its evolution in the current security context.

Today, the United States is advancing a new set of strategic concepts, referred to as "integrated deterrence," to better account for an increasingly competitive security environment in which Russia and China are utilizing comprehensive, multidomain, and multilayered defense strategies and highly interrelated strategic military technologies to challenge the United States and its allies.[6] As U.S. defense officials have made clear, however, this deterrence strategy goes beyond taking an integrated approach to technical domains and weapons systems, striving to better integrate strategic deterrence efforts with allies and partners in Europe and Asia, many of which are pressing for renewed assurance of U.S. extended deterrence while also calling for renewed efforts at collective risk reduction and arms control.

While many of the definitional and scoping issues associated with integrated deterrence remain under development, some of the foundational aspects of such a strategy are clear. Integrated deterrence marks a movement away from stovepiped approaches in which strategic deterrence rests exclusively on nuclear weapons. Instead, integrated deterrence recognizes the fundamental need to deter war and attendant escalation between nuclear-armed states, not just nuclear use. In part, this requirement is driven by the wider range of strategic technologies and domains, including space, cyber, advanced conventional capabilities (e.g., hypersonic delivery systems and missile defenses), and a host of gray

zone tactics and operations, for which new deterrence approaches and tools are needed. While the importance of better integrating deterrence strategy is widely appreciated, the very broad scope and complexity of integrated deterrence will inevitably open new stability risks and challenges. These complexities include reduced clarity about thresholds, triggers, redlines, and consequences for deterrence failure, as well as concepts of vulnerability and superiority, across such a diverse set of threats, actors, and activities.

As such, principles of stability and risk reduction will remain essential drivers of arms control even in an integrated deterrence framework. By enhancing stability, reducing arms racing, and enabling crisis transparency and communication, arms control may take on even greater importance in a strategy as broad and complex as integrated deterrence.

By enhancing stability, reducing arms racing, and enabling crisis transparency and communication, arms control may take on even greater importance in a strategy as broad and complex as integrated deterrence.

Facing a Resurgent Russia

Russia's steady expansion of nuclear-capable delivery systems and large inventory of sub-strategic nuclear weapons that fall outside of arms control or other regulatory structures highlight the gap between growing "arms" and shrinking "controls." The 2021 Annual Threat Assessment by the Directorate of National Intelligence (DNI) stated that Russia will remain the "largest and most capable WMD rival to the United States for the foreseeable future."[7] Furthermore, Russian nuclear weapons modernization is roughly 80 percent complete and boasts a range of novel nuclear weapons systems, including the deployed Avangard hypersonic glide vehicle, designed to evade missile defenses; Skyfall, a nuclear-powered, ground-launched nuclear-armed cruise missile (currently in development); the Poseidon nuclear-powered, very-long-range nuclear-armed torpedo (currently in development); and the deployed dual-capable ground-launched cruise missile.[8] While the New Strategic Arms Reduction Treaty (New START) between the United States and Russia limits the number of deployed strategic nuclear warheads and deployed strategic delivery systems through 2026, many of these new systems remain outside the controls of New START.

Qualitative and quantitative expansion of strategic systems, however, is not the only challenge for future U.S.-Russia arms control. Russian declaratory policy and concepts of nuclear use are opaque and uncertain. Russia's nuclear doctrine has been a source of debate within the U.S. arms control community for years, centering around whether and under what conditions Moscow might use nuclear weapons in hopes of successfully terminating a conventional regional conflict along the periphery of the North Atlantic Treaty Organization (NATO) without escalating to a larger nuclear exchange. Russian officials have consistently refuted the existence of an "escalate to de-escalate" or "escalate to win" doctrine. Western analysts are sharply divided over interpretations of Russian nuclear doctrine,

but it is clear that Russian strategy does include the potential first use of nuclear weapons in "dire circumstances."[9] In June 2020, Russia released an unclassified policy document, "Principles of State Policy of the Russia Federation in the Sphere of Nuclear Deterrence," which outlines Russia's basic principles on nuclear deterrence, including situations in which nuclear weapon use could be allowed, a statement of launch under warning from ballistic missile attacks, and the assertion that any attack on Russia's nuclear command and related infrastructure justifies a nuclear response.[10] Even so, many unanswered questions remain, suggesting that new risk reduction measures could play an important role in managing aspects of competition between the United States and Russia.

Russian advances in strategic systems have been accompanied by more aggressive regional activities, which have posed a continuing concern to the United States, NATO, and other partners in the region. Since 2014, civilian and military cooperation at the NATO-Russia Council has largely been suspended in response to Russia's "military intervention and aggressive actions in Ukraine, and its illegal and illegitimate annexation of Crimea," according to NATO.[11] Moreover, in early 2021, Russia deployed military forces on the eastern border of Ukraine in response to increased conflict between Ukrainian forces and Russian-backed separatists. While Russia announced a military pullback in April 2021, tensions in the region have remained high and were further heightened in October 2021 when NATO expelled eight members of Russia's mission, stating they were "undeclared Russian intelligence officers."[12] Russia responded by halting all activities of its diplomatic mission to NATO and declaring that all staff at NATO's military mission in Moscow would be stripped of their accreditation and that the information office would be closed.[13] At the same time, continued Russian regional intervention in Belarus, increased engagement with Turkey, and assertive posturing and approach operations along NATO's air and sea periphery further complicate regional dynamics and strain future arms control agreement negotiations.

Russia's increasingly aggressive posture in the space and cyber domains has prompted renewed interest in incorporating these areas into strategic risk reduction efforts. According to a public report by the U.S. Defense Intelligence Agency, Russia views space as a warfighting domain and has developed and tested direct-ascent anti-satellite weapons capable of destroying satellites in low Earth orbit (LEO).[14] Moreover, as a result of Russia's antagonistic behavior in space, primarily through unusual maneuvering of its satellites in geostationary orbit, France claimed Russian satellites were attempting to engage in space-based espionage.[15] The unusual maneuvering has renewed international focus on space norms and laws, which struggle to differentiate normal rendezvous and proximity operations from aggressive or hostile ones.[16] Increased Russian space operations, especially development of counterspace weapons, could also have adverse effects on critical early-warning and communication infrastructure and a myriad of space-dependent warning, detection, and operational capabilities. Russian cyber operations also pose a direct deterrence challenge, particularly given their use to target critical infrastructure. The May 2021 ransomware attacks on the Colonial Pipeline and JBS meat plant, both part of U.S. critical infrastructure, resulted in a scramble for oil and meat and demonstrated the potential vulnerability of U.S. strategic assets.[17]

These tactics also reflect Russia's increased use of sub-conventional operations in the "gray zone," the space between routine statecraft and open warfare, in order to exert influence and shape the geopolitical landscape in ways that better serve its interests.[18] Russia's gray zone activities include information and disinformation operations, offensive cyber activities, provocative space operations, targeted assassinations, and aggressive regional activities, including coercion and intimidation.

Military vehicles carrying DF-5B intercontinental ballistic missiles participate in a military parade at Tiananmen Square in Beijing on October 1, 2019, to mark the 70th anniversary of the founding of the People's Republic of China.

Photo: Greg Baker/AFP via Getty Images

Competing with a Rising China

China's overall nuclear force, publicly estimated around 250 warheads, includes strategic capabilities such as dual-capable missiles, all of which are entirely unregulated from an arms control perspective.[19] Worryingly, reports suggest that China is engaged in a major strategic buildup of its nuclear and other strategic forces. A 2021 Department of Defense report states that China's nuclear warhead stockpile could reach up to 700 deliverable warheads by 2027 as China expands and modernizes its nuclear forces.[20] Three open-source investigations, published in June, July, and August 2021, revealed that China is building new nuclear missile silo fields in Yumen, Hami, and a potential site in Haggin Banner.[21] According to the reports, approximately 250 new silos are under construction, constituting the "most extensive silo construction since the US and Soviet missile silo construction during the Cold War."[22] In addition, open-source analysts have identified construction of a new tunnel and roads at Lop Nur, the former Chinese nuclear test site.[23]

At the same time, China is pursuing a nuclear triad with the development of a nuclear-capable air-launched ballistic missile and improved ground- and sea-based nuclear capabilities.[24] The 2021 DNI Annual Threat Assessment states that China's nuclear modernization will result in a future nuclear missile force that is more survivable, diverse, and on higher alert than at present. Moreover, China's nuclear weapons will be designed to "manage regional escalation and ensure an intercontinental

second-strike capability."[25] In testimony to the Senate Armed Services Committee in April 2021, Admiral Charles Richard, commander of U.S. Strategic Command, stated that China's nuclear modernization and development of new capabilities, to include road-mobile intercontinental ballistic missiles (ICBMs), solid fuel ICBMs, strategic bombers, and a dedicated nuclear command and control capability, make it a significant strategic and pacing threat for the United States.[26] In August 2021, reports indicated that China may have tested a space-based hypersonic missile. While the precise purpose of the tested system is unclear, a number of analysts suspect China was testing a fractional orbital bombardment system (FOBS) that would launch a hypersonic glide vehicle into orbit. These recent tests underscore Admiral Richard's concerns and raise questions about whether U.S. defense and warning systems can detect and track such weapons.[27]

China's traditional nuclear doctrine is based on the premise of a minimum deterrent and a "No First Use" (NFU) declaratory policy.[28] China balances the size of its nuclear arsenal with emphasis on strategic ambiguity and a reluctance to engage in many of the transparency measures that have become hallmarks of the U.S.-Russia relationship, such as on-site inspections and data exchanges. China sees few incentives to join arms control agreements that it believes will enable adversary counterforce capabilities, cap strategic programs at levels below those of the United States and Russia, or introduce strategic constraints in otherwise unregulated areas such as space, cyber, or advanced conventional strike. Nevertheless, China's expanding strategic capabilities, including qualitative and numerical expansion of its nuclear force and dual-use, long-range delivery systems, are unfolding at a time when the expert community is increasingly divided about China's intentions to strictly adhere to a declared NFU policy, especially in complex crises.[29]

China also seeks to exploit the sub-conventional or pre-war space to secure its interests and expand its influence by employing gray zone and related tactics to test and, in some cases, subvert the rules-based international order and its institutions. These activities include provocation by state-controlled forces, economic coercion, influence and information operations, and offensive cyber and space activities.[30] Provocation by state-controlled forces encompasses China's militarization of the South China Sea—China's island-building activities and claims of sovereignty in the surrounding waters pose security considerations across East Asia because of the flow of oil and commerce through the South China Sea's shipping lanes. China's economic coercion includes President Xi Jinping's Belt and Road Initiative (BRI), which was established to increase China's trade connectivity, reduce surplus domestic industrial capacity, and shape economic dependencies such that other countries would be reluctant to intervene in Chinese affairs.[31] China has also been known to use economic sanctions for coercive purposes, and while most of these tactics do not have a nuclear component, they can complicate the United States' perception of stability and risk.[32]

Like Russia, China seeks to compete aggressively in the space and cyber arenas. A report by the U.S. Defense Intelligence Agency assessed that China could use cyber capabilities to support military operations by collecting technical and operational information for intelligence and potential operational planning; establishing information dominance and "constraining adversary actions by targeting command and control (C2), command, control, communication, computers, intelligence surveillance, and reconnaissance (C4ISR), logistics, and commercial activities"; and as a force multiplier when coupled with conventional capabilities.[33] To date, China has proved its hacking capabilities through an attempt to hack U.S. satellites in 2008, an attack on the National Oceanographic and Atmospheric Administration's satellite information and weather systems in 2014,

a hack of the U.S. Office of Personnel Management in 2014 and 2015, and a successful transfer of 22 gigabytes of data from NASA to a Chinese IP address in 2019.[34] While there has been a moderate decrease in economic cyber espionage since the 2015 agreement between the United States and China, which included a commitment by both sides to refrain from supporting cyber-enabled theft of intellectual property, there has been no movement to further restrict cyber operations or increase transparency.[35] The 2021 DNI Annual Threat Assessment determines that China's cyber capabilities present a growing influence threat to the United States.[36] Unchecked cyber capabilities raise concerns of the vulnerability of critical infrastructure to hacking while also raising questions on the implications for arms control if hackers were to target individuals and institutions responsible for the negotiation, implementation, and verification of agreements.

In addition, China has increased its use of aggressive space operations. The 2020 Department of Defense report on China's military power found that China's space enterprise continues to mature rapidly, with China declaring space a "critical domain in international strategic competition."[37] General James Dickinson, commander of U.S. Space Command, identified China's space program as the pacing challenge for the United States. General Dickinson further stated that while China maintains its public stance against the weaponization of space, it has continued to build military space capabilities.[38] China has significant kinetic physical counterspace capabilities, including direct-ascent anti-satellite weapons which can reach targets in LEO and geostationary orbit (GEO).[39] China has also developed and launched satellites that could be used for co-orbital counterspace activities, though the purpose of these new satellites is unclear. There is also concern that China has the conventional capability to hold ground stations that control satellites at risk during conflict through ballistic missiles, cruise missiles, or long-range strike aircraft.[40] Moreover, China is increasing its development, testing, and fielding of non-kinetic physical and electronic counterspace weapons with the capability to dazzle or blind satellites as well as jam and spoof.[41]

Aligning with Allies

The evolving security environment has implications for extended deterrence and assurance as well as for allies' views of arms control. Renewed strategic competition and technological advances by Russia and China have increased anxiety among many of the United States' allies in Europe and Asia. This has led to renewed calls for strengthening extended deterrence and a reprioritization of rebuilding credibility with allies within U.S. security policy. While the Biden administration has clearly emphasized rebuilding alliance relationships, navigating this terrain remains challenging. U.S. withdrawal from Afghanistan in August 2021 prompted outrage from many European allies, which perceive that they are not as important to Washington as they used to be.[42] Additionally, while many security partners understand and support renewed U.S. attention on China, some of the steps toward prioritizing the Indo-Pacific region have proved bumpy for Washington. In the wake of the Australia-UK-U.S. submarine agreement (AUKUS), for example, some European leaders questioned the United States' loyalty to transatlantic cooperation and collective security.[43] In Asia, concerns from Japan and South Korea about perceived inequities resulting from the AUKUS arrangement remain to be assuaged.

Senior officials have made clear that allies are a central component of integrated deterrence. In a September 2021 call with Baltic allies, for example, Dr. Colin Kahl, undersecretary of defense for policy, described integrated deterrence as a response to an increasingly complex and changing landscape, which would require response across domains and "crucially alongside our allies and

partners."[44] And in a speech in Singapore, Defense Secretary Austin described integrated deterrence as "using every military and non-military tool in our toolbox in lockstep with our allies and partners. Integrated deterrence is about using existing capabilities, and building new ones, and deploying them all in new and networked ways—all tailored to a region's security landscape and growing in partnership with our friends."[45]

But calls for increased confidence in U.S. security guarantees also come amid increasing pressure, particularly among NATO members, to demonstrate progress toward nuclear risk reduction and additional arms control. With the collapse of arms control agreements, such as the Intermediate-Range Nuclear Forces (INF) Treaty, many European countries have initiated their own risk reduction efforts over the past five years, such as the Stockholm Initiative, leadership in a Creating an Environment for Nuclear Disarmament (CEND) subgroup, and the German government's initiative on the future of arms control, in the hopes of generating new ideas, encouraging renewed efforts at arms control, and giving greater voice to European partners in future arms control debates. While many of these European partners would not be interested in joining treaty-based strategic agreements, they have shown an interest in a wider array of arms control measures and management tools. The Stockholm Initiative, for example, outlined a series of steps nuclear possessors might take to reduce nuclear risks, including expansion of hotlines, agreement that "a nuclear war cannot be won and must never be fought," and a P5 working group on developments in offensive and defensive systems and counterspace capabilities.[46]

Calls for increased confidence in U.S. security guarantees also come amid increasing pressure, particularly among NATO members, to demonstrate progress toward nuclear risk reduction and additional arms control.

European interest and leadership on arms control also provides an important release valve for pressure to show progress toward nuclear disarmament. One result of this pressure was the 2017 Treaty on the Prohibition of Nuclear Weapons (TPNW), which prohibits nuclear possession, testing, proliferation, assistance, the threat to use nuclear weapons (i.e., deterrence), and a multitude of other activities. While not supported by the governments of NATO member states, the TPNW enjoys considerable support among some European publics who might perceive nuclear weapons as the problem, not as a source of security. Support for the TPNW also runs strong among domestic constituencies in much of Asia, including close allies and partners such as Japan, Australia, and New Zealand.

But recent research has demonstrated that the United States' allies have complex views on arms control and disarmament. For example, while one survey found support among the Dutch public for membership in the TPNW, a more recent survey found that this support would be contingent on membership by nuclear possessors.[47] And another survey found that while the German public is skeptical about the military utility of U.S. nuclear weapons in Germany, there was widespread support for their removal if it was part of an arms control initiative.[48] Arms control has been an integral part of NATO security since the 1967 Harmel Report, which called for deterrence and détente, to

include dialogue and cooperation on arms control working in tandem.[49] For many allies, therefore, arms control has the potential not only to demonstrate leadership to domestic audiences on their commitment to nuclear disarmament and risk reduction but also to strengthen collective security as part of the alliance. In many of these countries, arms control not only complements deterrence but may also be essential to its long-term survival as the foundational concept of alliance security.

In terms of arms control, this means the United States will have to balance its continued reliance on nuclear weapons for allies' security with progress toward arms control and risk reduction measures in an increasingly complex and competitive strategic landscape. Going forward, European and Asian partners can be expected to press for greater participation in arms control agreements they believe directly impact their security regionally and globally. While this will not necessarily entail the participation of the United Kingdom or France in arms control agreements or the reduction of their nuclear weapons arsenals, internal and external pressures to engage more directly in risk reduction measures in a P5 context are likely to grow.

The United States will have to balance its continued reliance on nuclear weapons for allies' security with progress toward arms control and risk reduction measures in an increasingly complex and competitive strategic landscape.

2

The Evolving Technology Landscape

Challenges for Arms Control

Over the last 20 years, the world has witnessed the emergence of an increasingly dual-use, highly interconnected military technology landscape with a broader array of strategically significant capabilities. The Biden administration's Interim National Security Guidance, published in March 2021, for example, pointed to the "technological revolution that is reshaping every aspect of our lives," along with the ways that China and Russia are using their technological power to challenge the current international system.[50] This evolving technological landscape has three broad implications for arms control: (1) these technologies complicate strategic stability and risks of crisis escalation and arms racing; (2) many of these advanced technologies are used in both the civilian and military sectors, complicating the scope, applicability, implementation and verification of arms control measures more accustomed to regulating government-controlled technologies and practices; and (3) most of these technologies exist outside of existing arms control regulations, meaning legal mechanisms will likely struggle to incorporate them.

Advanced Technologies and Strategic Stability

Advanced technologies, such as artificial intelligence (AI) and hypersonic weapons, which can impact strategic stability, escalation risks, and crisis management positively or negatively, have become priority focus areas for a number of arms control initiatives. One common trait of many of these technologies is the increasing speed they contribute to targeting, decisionmaking, and launch-to-delivery strike times. This could speed up crisis escalation and increase risks of misperception. On the other hand, by speeding up data analysis and processing speeds, improving communications, and automating certain warning and targeting functions, such technologies can increase decision space and potentially reduce miscalculation risks.

Additionally, as discussed above, Russia and China are already pursuing many of these technologies as part of their nuclear modernization programs, which arguably has already prompted an arms race and an "action-reaction" cycle. All of these technologies are also rapidly evolving. Funding for AI, for example, more than doubled from 2017 to 2021.[51] One area where AI efforts are increasingly focused is on emotional intelligence, which has been largely absent in AI to date, with Huawei currently developing an emotional intelligence voice recognition software.[52] These developments, as in the biotechnology sector, were largely unimaginable until recently. Many of these technologies may have benefits for arms control, such as the potential use of AI in arms control inspection, but the impact of these technologies on strategic stability also complicates the way forward for arms control.[53]

Some of these capabilities are reflected in the trend toward more advanced, potentially dual-capable (conventional/nuclear) long-range delivery systems, including hypersonic glide vehicles, and increasingly capable missile and air defenses. Offense-defense competition, fueled by the numerical expansion and qualitative improvement of long-range strike capabilities and missile defenses is driving investment and competition in increasingly problematic ways. Unchecked, some of these advanced technologies could erode nuclear survivability, create incentives for crisis escalation, or complicate crisis management. Conventional capabilities, including advanced sensing and surveillance, have improved the range, precision, lethality, and stealth of conventional capabilities, raising the prospect of counterforce options and preemptive capabilities previously believed infeasible. Rose Gottemoeller has suggested that in the coming decades many of these advanced technologies could create a future "standstill conundrum" that "may render mobile missiles and submarines vulnerable to detection. . . . States will no longer be able to assure a nuclear response should they be hit by a nuclear first strike."[54] The potential for dramatic informational advantage through the combination of stealthy or remote platforms, highly capable quantum sensors, and AI-enabled data fusion and management has military and civilian leaders suggesting an age of information dominance and decision superiority may be imminent.[55] It is difficult to imagine, however, any state allowing such an advantage to proceed unchecked, which suggests information arms racing or targeted disablement or destruction of surveillance and warning assets could result.

Dual-Use Technology and Challenges for Arms Control

The use of these technologies by both civilian and military entities, with the commercial sector even representing their primary residence, can pose challenges for arms control, especially verification. For most emerging and potentially disruptive technologies, private actors, rather than governments, are the primary developers and drivers of innovation. In many cases, militaries are adapting technologies developed for civilian use to military purposes rather than the other way around. When aided by machine learning (ML) techniques, AI can incorporate massive amounts of data to make independent, intelligent decisions.[56] China is arguably the world leader in AI because of the amount of data it generates through its large population and because of its extensive use in domestic surveillance.[57] In addition to generating huge amounts of data, AI can also process data for intelligence collection and analysis, optimize military planning, and "revolutionize" warfare.[58] An April 2021 report by the U.S. National Security Commission on Artificial Intelligence points to the risks of China leveraging AI to launch cyberattacks and implement "intelligentized war" with better-connected systems.[59] The rapid growth in AI/ML-enabled military technology has prompted a cascade of reports and studies considering the potential for arms control-like efforts to rein in some of the more competitive and

risky applications for AI, especially in the nuclear arena.[60] In all cases, however, the broad availability and lack of public sector control make such initiatives challenging to implement. A related trait of these advanced technologies is that they are ubiquitous and used extensively in everyday life, including for military applications. Space and cyber are predominantly civilian technologies and domains on which global commerce, banking, communications, transportation and more all depend, even as they also involve essential military technologies as well as potential vulnerabilities.

Another example of advanced, dual-use, and highly disseminated technology is biotechnology, which is overwhelmingly powered by private entities.[61] Biotech research is vital for human health and safety, as was recently highlighted with the development of mRNA vaccines for the Covid-19 pandemic. At the same time, biotech applications such as CRISPER-Cas9, which allows for unprecedented ease and control of genome editing, could have implications for biological weapons, either by advancing human performance or in developing new offensive capabilities.[62] The current state of biotech was not envisioned when the Biological Weapons Convention (BWC) opened for signature in 1972, allowing for the possibility of this technology to be created outside the bounds of an international agreement. Furthermore, the Covid-19 pandemic is likely to increase biotech research and raise biosecurity risks while domestic and international rules struggle to keep up.[63] As a result, these new technologies might require changes in safety requirements to reduce risks of misuse or manipulation that are not captured by existing agreements. The example of biotech also highlights a bigger challenge of advanced technologies—balancing the potential benefits to humanity with the risks of misuse.

The rapid way in which these technologies are being developed, fielded, and updated is straining the ability of existing legal mechanisms and arms control institutions—often more rigid and slower to adapt—to keep up. Even in the case of the Chemical Weapons Convention (CWC), one of the most comprehensive, verifiable, and universally adhered to arms control treaties in existence, technology is challenging existing structures.[64] The CWC was designed with the voluntary dismantlement of industrial-scale, military-grade chemical weapons programs in mind, but, with the notable exception of North Korea, few if any such programs still exist. In reality, modern chemical weapons programs do not require production-scale facilities or large bulk quantities of agents or precursors. Instead, production at the research and development (R&D) level combined with on-demand surge capacity would be sufficient for almost all scenarios, especially given advances in chemical science and engineering and rapidly expanding usable chemical compounds outside of the CWC control regime.[65] More than 100 million new chemical substances have been created since the establishment of the CWC Schedules—growing by about 15,000 substances per day.[66] In addition, synthesizing precursor chemicals from simpler, unregulated, or domestically available ones grows easier by the day. Meanwhile, diffuse procurement networks and access points facilitate the ability to identify and deceive suppliers, especially with the growth of online directories and unregulated procurement sources. Finally, advances in R&D and production techniques, including in microfluidics, additive manufacturing, and AI, are enhancing the speed, precision, and ease of concealment of chemical weapons activities.

But states might lack both the political will and tools to apply arms control to advanced technologies. Many of these technologies are still under development, and both states and private companies might be unwilling to subject them to limits that could curtail future economic or military advantage. Arms control limitations could come at the cost of technological competition, particularly in the early stages of development when a technology's full potential has not been realized or applications are

still under development, such as with emotional intelligence in AI. Similar challenges have existed with arms control efforts in the chemical and biological weapons arenas, but progress may be feasible over time with close consultation and cooperation between public and private actors. At the same time, traditional verification tools, such as inspections, may prove infeasible either because controlled capabilities are inaccessible or privately held. For example, how would the United States and Russia inspect each other's offensive cyber capabilities? And how would they distinguish offensive from defensive cyber capabilities (what Ben Buchanan identified as the "cyber security dilemma")?[67] These challenges—including the impact on strategic stability, the dual-use nature of many technologies, and the political and practical limits of arms control mechanisms—will have to be considerations in developing arms control in an integrated deterrence environment.

The rapid way in which these technologies are being developed, fielded, and updated is straining the ability of existing legal mechanisms and arms control institutions—often more rigid and slower to adapt—to keep up.

3

The Evolving Information Ecosystem

Arms Control in the Digital Information Age

Today, arms control exists in an information ecosystem which is highly digitized and easily weaponized. This combination of factors will lead to additional stresses on the availability of reliable, transparent, and accurate information necessary to support successful arms control implementation. Although the growing accessibility and diffusion of online platforms and digital tools have democratized information, they have also contributed to its manipulation and misuse while undermining traditional sources of credible and authoritative information, including sources such as government-held intelligence and national technical means (NTM) of surveillance and monitoring. The evolving information ecosystem, specifically the potential benefits and challenges for accessing, processing, analyzing, altering, and disseminating large volumes of information, is poised to change the nature of arms control.[68] This complex and highly dynamic information environment will potentially transform how agreements are negotiated, monitored, verified, and enforced, not to mention altering roles and responsibilities along the way. Advanced technologies, such as AI and quantum computing, among others, will also present both challenges and opportunities for future monitoring and verification activities, particularly in terms of confidence in data.

Influence and Information: Arms Control in the Disinformation Age

Arms control agreements and institutions, such as the CWC, have been a target for state-based influence operations, including disinformation and digital media manipulation, to distract, disrupt, dissuade, distort, or influence decisionmaking in the targeted states or international entities.[69] Furthermore, weaponized social media and information sabotage can be used by states or non-state actors with competing agendas to discredit the negotiation, implementation, and verification of arms control.

Influence operations are a key component of Russian, and to a lesser but growing extent Chinese, gray zone strategies and a perceived source of competitive advantage. Influence operations encompass state-directed activities to limit a target country's ability to interpret a situation and act effectively in its own interests by manipulating the information environment. This can occur at either the micro or macro level in ways that are often covert, unattributable, or deniable.[70] Such operations are integrated into military doctrine and intended to be deployed in peacetime and in crisis. While the use of disinformation through influence operations is not necessarily a new tactic, the rise of online platforms and digital tools as well as the growing accessibility of the internet has allowed for the increased penetration and spread of disinformation. As the United States, Russia, and China vie for influence on the world stage and seek to shape international narratives in ways that favor their strategic objectives, this information ecosystem will intensify arms control competition, complicate and transform how arms control is implemented, and open existing and future arms control agreements and their associated structures and institutions to information-related attack and disruption.

This complex and highly dynamic information environment will potentially transform how agreements are negotiated, monitored, verified, and enforced, not to mention altering roles and responsibilities along the way.

Russian influence operations have been particularly active in the chemical weapons arena, offering a degree of insight into the activities and tactics that might be expected in other arms control contexts. These activities have included the counternarrative messaging associated with the use of chemical weapons in Syria; the use of Novichok agents in an assassination attempt on former Russian intelligence agent Sergei Skripal and his daughter; a similar attack on prominent opposition politician Alexei Navalny; promotion and amplification of so-called OPCW (Organisation for the Prohibition of Chemical Weapons) whistleblowers; cyberattacks targeting the OPCW; and disinformation campaigns. Moreover, reports indicate that the Russian Military Intelligence Service—known as the GRU—has an elite unit skilled in subversion, sabotage, and assassination that is credited with the poisoning of an arms dealer in Bulgaria, a failed coup in Montenegro, the assassination attempt on the Skripals, allegedly offering bounties to Afghan militants to kill U.S. troops, an explosion in a Czech arms depot, the attempted assassination of Navalny, and disinformation campaigns about Covid-19.[71]

These actions are indicative of the types of tactics that could be applied to arms control structures. For example, Russia might use its cyber operations to undermine the legitimacy of institutions and organizations involved in arms control, manipulate or discredit verification information, or target arms control staff, negotiators, or national representatives through doxing, ransomware, bribery, or other coercive approaches. Russia attempted to do this in April 2018, when four GRU agents were apprehended trying to hack computers at the OPCW.[72] At the time, the OPCW was investigating the poisoning of Sergei Skripal and the 2018 Douma chemical weapons attack in Syria, which Russia claimed was a false flag. In October and November 2021, Russia again attempted to use an influence campaign in response to a formal request by 45 CWC states parties to "clarify and resolve" unanswered

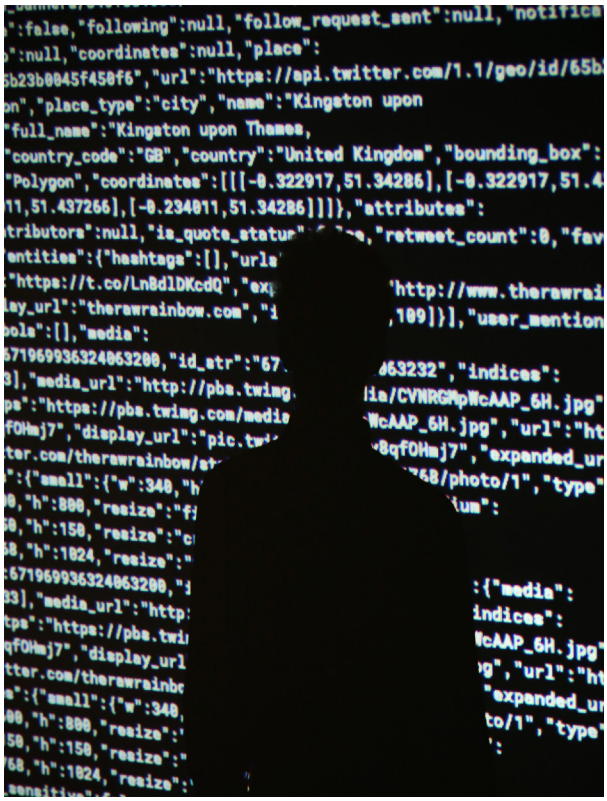
questions regarding Russia's handling of the Navalny poisoning.[73] Russia responded by providing a lengthy note verbale that did not answer the questions posed and instead accused the questioning parties, mainly Germany, France, and Sweden, of staging the evidence and failing to act impartially.[74] The Russian news agency TASS produced articles to support Russian claims and spread disinformation, which take up 7 of the top 10 searches for "OPCW news" on Google.[75] Russian influence operations test the West's ability to defend and enforce a rules-based international order. While these sub-conventional operations do not necessarily have a nuclear component, they have complicated the West's perceptions of stability in ways largely unregulated by the international community.

Chinese influence operations also seek to change existing narratives or sow confusion and doubt. The 2021 report on China's military power by DoD assessed that China believes controlling the information space and achieving information dominance is critical to countering third-party intervention in conflict.[76] Experts also claim that China is learning from other countries and adopting effective tactics for influence operations.[77] In 2020 and 2021, China used disinformation campaigns on Twitter to undermine protestors in Hong Kong and sow doubt about the origins of Covid-19. The increase in the number of Chinese-affiliated accounts and output of tweets marks a turn in China's social media disinformation tactics, becoming more aggressive and conspiratorial than in the past. China's development and adoption of Russia's information operation tactics could pose additional challenges to future arms control.

The use of disinformation to undermine arms control structures, institutions, and mechanisms poses a large and growing challenge to future arms control. In particular, the falsification or manipulation of verification data or analysis will be a particularly novel challenge in future arms control agreements, especially as detection and attribution of such actions grow increasingly difficult. Manipulated information could be used to raise questions about a country's compliance with an arms control agreement, forge or fake a treaty violation, cover up or hide a violation, or cause confusion about a state's weapon development. Traditional verification and compliance regimes look at potential concealment activities, but if disinformation is being used to obfuscate information, this may require a new approach to verification—specifically in the evaluation and resolution phases—which prioritizes digital forensic capabilities. Information sabotage will have major implications for arms control agreements if international institutions and individuals responsible for negotiations, verification, and compliance decisionmaking are targeted by hackers or digital operatives to either manipulate outcomes, distort and extort information, or break trust in the system.

Implications of Open-Source Analysis and Data

State actors are not the only players of note in the new information ecosystem. The days of proprietary and private official sources and processes as an exclusive means of arms control monitoring and verification—particularly in the form of national intelligence—may be drawing to a close. The explosion of international open-source investigation and analysis groups outside the government, such as Project Sandstone, Bellingcat, the Center for Advanced Defense Studies, the Open Nuclear Network, and many others, will potentially transform not only how verification is done but also who does it. Open-source information and analysis can and should be leveraged when accurate and accessible. Indeed, in some cases, open-source intelligence may present a potential alternative for some future arms control arrangements in which intrusive monitoring inspections might not be agreeable or desirable. In addition to less-intrusive inspections, the nongovernmental open-source community could aid



A staff member stands in a projection of live data feeds from (L-R) Twitter, Instagram, and Transport for London by data visualisation studio Tekja at the Big Bang Data exhibition at Somerset House on December 2, 2015, in London, England.

Photo: Peter Macdiarmid/Getty Images for Somerset House

governments in collection of data, providing greater access, transparency, and independence on matters of compliance.

Nongovernmental open-source information also provides support for governmental analysis with publicly available and explainable methods. This is particularly helpful in cases in which national intelligence cannot be shared. Open-source information can be leveraged to debunk weaponized information aimed at undermining verification and compliance. Organizations such as Bellingcat and the Datayo Project have produced impactful open-source investigations into chemical weapons violations, Russia's GRU network, and Iran and North Korea's nuclear programs.[78] As individuals not tied to a government and bureaucratic process, open-source analysts are able to quickly analyze and publish findings, sometimes long before official government findings are concluded and made publicly available. The analyses produced by open-source organizations have substantially increased response time, public awareness, transparency, and accountability.[79] However, the rise of open-source information could also pressure governments to respond prematurely to reports and violations while also taking the option of closed-door diplomatic discussions off the table.[80]

The rise of open-source investigations gives nongovernmental entities greater power and voice and could affect perceptions of validity, either favorably or unfavorably. Credible and independent open-source analysis can be used to counter disinformation and support independent reliable verification, but states may also create or leverage open-source authorities to advance their own counternarratives. For example, the Russian government has issued satellite images of bombings in Syria to support "false flag" claims against entities such as the White Helmets. At the same time, state-backed media outlet RT has created a website that mimics Bellingcat used for "digital verification."[81] Efforts to protect and validate sources have struggled to keep up with the rapid growth of open-source analysis, leaving the arms control community with no national or international guidelines or even best practices for policing the analysis and reliably distinguishing between reputable sources, state-sponsored propaganda, and conspiracy-driven fake news. While some open-source organizations, such as the Datayo Project, have created a code of ethics to guide operation, it only applies to its employees.[82] No common set of standards, let alone processes for their enforcement, exists across the open-source community of analysts and scholars.

This emerging information ecosystem, particularly in the form of highly competitive open-source analysis and investigation, will inevitably impact the role of NTM—nationally controlled ground, space, airborne, or even underwater sensors—in monitoring and verifying compliance with arms control agreements.[83] NTM have been an essential component of robust monitoring and verification regimes and, since the Anti-Ballistic Missile Treaty, are largely protected from interference under treaty language. This protection has continued through New START and is understood to encompass the entirety of U.S. and Russian national security space constellations.[84] However, new technology and the evolving information ecosystem might mean next-generation arms control agreements will have to reexamine the role of NTM, both in terms of the range of capabilities that constitute NTM and in the way that such information is shared and distributed. It is possible to expect some new technologies, such as AI, to be included in next-generation NTM. A recent interim study by the National Academies of Sciences, Engineering, and Medicine found that the amount of open-source data is growing rapidly, and monitoring, detection, and verification entities should "consider open-source information/data as an important adjunct to NTM that can possibly corroborate or enhance NTM data sources."[85] The inclusion of open-source investigations for verification could require information gathered by NTM to be shared beyond the proprietary and private official sources that characterized previous verification regimes. Moreover, NTM resiliency will also depend on strong defenses against attack, resulting in disablement or distortion that could reduce the reliability of NTM. For example, NTM could be hacked or exploited through increased cyber capabilities or simply disputed or contradicted through alternative, sometimes fictional or faked sources. The classified, sensitive, or proprietary nature of NTM could impair governments' ability to counter and refute such attacks.

Additionally, there are risks to outsourcing sensitive national intelligence-gathering practices to open-source analysts without clear lines of authority or accountability to national or international bodies. The need for independent and reliable implementing bodies has been a driving force behind the creation of international arms control institutions that can act as semi-autonomous organizations specifically for verification and compliance monitoring, such as the International Atomic Energy Agency (IAEA) and OPCW. Similarly, the Comprehensive Test Ban Treaty built in a robust verification regime that includes an international monitoring system, international data center, and a global communications infrastructure to monitor and track any nuclear weapons test, all of which is centralized in an international body: the Comprehensive Test Ban Treaty Organization.[86] Future agreements could build similar types of organizations or bodies that use open-source analysis and operate beyond national intelligence to ensure verification and compliance.

4

Evolving Concepts of Escalation and Stability

Integrated Arms Control and Risk Reduction

While arms control may have roots in humanitarian and ethical initiatives, it evolved over the twentieth century into a tool that could work in tandem with deterrence. Some of the first attempts at multilateral arms control in the twentieth century included the Hague and Geneva Conventions, which sought to reduce the humanitarian consequences of warfare by curbing weaponry seen as particularly indiscriminate or as having disproportionate effects, especially in terms of the impacts on unarmed or vulnerable civilians. By banning or eliminating certain types of weapons and behaviors from the battlefield, countries could avoid ceding strategic advantage to an adversary while lowering the costs and collateral damage of indiscriminate warfare. The nuclear age and subsequent Cold War, however, ushered in new forms of arms control which recognized that escalatory pressures, whether through unregulated competition, mistakes and miscalculation, or crisis mismanagement, could lead to deterrence failure and nuclear use.

By reducing incentives for nuclear first use and lowering risks of miscalculation, arms control during the Cold War depended on limited cooperation to reinforce more stable deterrence even if the elimination of nuclear weapons might prove unrealistic or infeasible. For this to work, however, adversaries needed at least a tacit understanding of how a crisis might unfold and what escalation might look like, including triggers and thresholds for nuclear use. Fear of direct large-scale escalation between two near-peer adversaries emanating from perceived military advantage, uncontained conventional aggression, or catastrophic miscalculation animated the shape and scope of bilateral strategic arms agreements between the United States and the Soviet Union (and now Russia). The most successful and enduring arms control measures were those that reinforced second-strike stability at lower numbers, promoted cooperation and communication between peer adversaries, and encouraged transparency in ways that reduced arms racing pressures. Both

deterrence and arms control agreements relied implicitly on two essential theoretical principles of escalation and stability:

1. Escalation would most likely unfold in a series of quasi-predictable steps of increasing risk and intensity, epitomized in Herman Kahn's 44-rung escalation ladder, which offered opportunities for managing and reducing escalation risks.

2. Physical and conceptual separation between conventional and nuclear forces and related capabilities could reinforce perceived firebreaks and lower the risk of nuclear escalation. In fact, if sufficiently robust, such firebreaks could lead to the "stability-instability paradox," which posits that as strategic stability is strengthened, the likelihood of conventional conflict grows because the attendant nuclear escalation risks have been moderated.

Today's strategic security environment is far more complex and multifaceted than the dyadic days of the Cold War and far more competitive than the immediate post–Cold War years, calling into question assumptions about escalation and how a crisis might unfold. First, the potential battle space is more multidomain and more technologically integrated across the air, land, sea, space, and cyber arenas, all of which may achieve a degree of strategic effect. For example, any attack on conventional command and control infrastructure, including an array of space-based assets, could also disable or disrupt vital nuclear command and control systems.[87] Such an attack during a conventional conflict might easily be perceived as a precursor to a nuclear first strike.

Relatedly, potential conflicts are also multidimensional, blurring the lines and diminishing firebreaks between echelons of conflict, particularly as conventional and nuclear capabilities become more entangled and advanced conventional capabilities become more strategic in their effects. Whether in terms of advanced missile defenses, hypersonic delivery systems, or the rapid proliferation of space-based strategic assets, technological advances create asymmetries that could embolden adversaries to escalate through non-nuclear means, believing they can avoid any "redlines" while pursuing a strategic advantage. It is in these areas where the most pronounced arms racing pressures are already being felt. In the absence of discernable firebreaks along the conventional-strategic interface, redlines and thresholds will inevitably be fuzzier.

Deliberate conventional escalation is already a serious concern in the South China Sea, where China's expansive territorial claims are policed by an increasingly large and effective naval presence as well as close control of and interaction with nonmilitary Chinese fishing and transport vessels. China "may increase the risk of one side seeing a strategic or political benefit from escalating such a clash deliberately."[88] As rapidly advancing U.S., Russian, and Chinese conventional capabilities become increasingly complex, integrated, capable, and co-mingled, first-strike advantage and second-strike vulnerability may reemerge as a strategic stability challenge. Conventional arms racing may also take on greater strategic significance as states seek to integrate new technologies into their conventional forces and further narrow the gap between conventional and strategic warfare. Advances by one country might also prompt a response in a classic "action-reaction cycle" involving both offenses and defenses. The nuclear shadow is inescapable—what starts as a conventional conflict may quickly create incentives for nuclear coercion or even use, especially if a party concludes that limited nuclear use may be possible without triggering an all-out nuclear exchange.

Moreover, escalation risks are not limited to the upper echelons of conflict. Sub-conventional or gray zone conflicts are unlikely to offer a risk-free alternative to conventional warfare, especially if such

activities achieve strategic effects or shift the strategic balance between competing states. For example, deliberate or inadvertent escalation could result from gray zone activities in Eastern Europe that usurp national authority, Chinese operations in the South China Sea that press territorial claims well beyond internationally recognized boundaries, or a Russian invasion of allied airspace or maritime areas in ways that lead to hostile military interactions—all of which would occur under an unavoidable nuclear shadow.

As a result, the nature of conflict, crises, and the escalatory pressures that shape them is subject to change. If Cold War stability concepts drew heavily on ladders and firebreaks to define nuclear crises and escalation, contemporary deterrence failure may more closely resemble "wormholes"—sudden, possibly temporary openings in the fabric of deterrence that allow for accelerated and unpredictable escalation risks. Future conflicts are unlikely to unfold in a clear linear or stepwise fashion with a distinction between pre-conflict and conflict termination. Neither is a clear distinction between nuclear and non-nuclear crises sustainable when conventional and nuclear capabilities are highly co-mingled, capable of more diversified strategic effects, and increasingly vulnerable to detection, disruption, or disablement.[89] Rather, "wormhole escalation" can unfold across domains, which are blurred, and can quickly jump from one echelon of conflict to another.

If Cold War stability concepts drew heavily on ladders and firebreaks to define nuclear crises and escalation, contemporary deterrence failure may more closely resemble "wormholes"—sudden, possibly temporary openings in the fabric of deterrence that allow for accelerated and unpredictable escalation risks.

This highly entangled, multidomain risk landscape suggests that new approaches to arms control will be needed. Integrated deterrence strategies can only provide partial answers to this complex and multidimensional strategic challenge. In fact, in a deterrence framework that is much larger and more comprehensive than traditional nuclear deterrence, gaps and weaknesses that create the potential for wormhole dynamics are more likely, not less. Likewise, the very nature of integrated deterrence erodes the utility of firebreaks in arresting stability risks as capabilities grow more entangled. Furthermore, the rising peer status of China, accompanied by increasingly capable regional nuclear actors, suggests multi-actor and multifocal approaches will need to replace traditional bilateral ones.

And yet, simply reverting to multilateral, humanitarian-focused arrangements of the past is unlikely to address the complex stability questions that arise from a security environment shaped by strategic competition and driven by increasingly ubiquitous and dual-use technology. While the mechanisms and modalities of arms control have yet to catch up to this emerging reality, the fundamental objectives of strategic arms control remain—preventing war and attendant escalation that could lead to nuclear use. Therefore, it is in identifying and mitigating deterrence gaps and risks that future arms control may prove most useful by focusing on arms control's role in preventing conflict in the first

place as well as costly arms races that might incentivize nuclear first use or crises that can rapidly escalate. In this way, rather than seeking to impose numerical constraints on specific technologies, states might prioritize arms control efforts that target specific behaviors of concern, regardless of the technological capabilities involved, and explore a wide range of arms control modalities to reduce the risks of arms racing and improve crisis stability.

Some potential priorities for crisis management in an integrated arms control framework could include reducing the risks of decision interference, such as deepfakes, autonomous systems that could accelerate decisionmaking, and a breakdown in strategic firebreaks. Arms control might address these risks in a variety of ways. For example, arms control agreements might prohibit deepfakes or establish cyber and space-based "no go" zones designed to support risk reduction in the decisionmaking arena. And to address the multidomain nature of these risks, a renewed focus on conventional arms control should seek to contain and manage crises at lower echelons of conflict. In particular, close-proximity approach operations among space-, air-, and sea-based assets can easily escalate. With these priorities in mind, both arms control and deterrence can be tailored as needed, drawing on a range of mechanisms and tools.

States might prioritize arms control efforts that target specific behaviors of concern, regardless of the technological capabilities involved, and explore a wide range of arms control modalities to reduce the risks of arms racing and improve crisis stability.

5

Integrated Arms Control

The Way Forward

Traditional bilateral strategic arms control mechanisms alone are insufficient to address the risks of escalation and arms racing in the current security and technological environment. New START is the last remaining formal mechanism governing the balance of strategic forces between the United States and Russia and is due to expire in February 2026. Multilateral structures, such as the CWC and BWC, are under pressure as they manage increasingly competitive dynamics and enduring verification and compliance challenges. These fora are straining to address the range of technical challenges and risks that have emerged since the agreements came into force. Following the recent demise of the INF Treaty and the Open Skies Treaty, observers are justifiably concerned that arms control agreements are a thing of the past.

And yet, the prospects for future arms control, if reimagined to account for the new risks to strategic stability in a highly complex, multipolar security environment and the requirements of a more integrated deterrence strategy, need not be bleak. In today's strategic landscape, arms control sits between competition and cooperation. States participate in arms control to help manage a competitive relationship and reduce associated risks, such as arms racing. At the same time, arms control offers a mechanism for cooperation that can reduce escalatory risks in crisis and conflict. Increasingly, arms control may also play important roles in helping the international community cooperate multilaterally to ensure societies benefit from scientific and technological advances while minimizing risks of misuse, work collaboratively to minimize global threats such as pandemics, and engage regionally to reduce both conventional and strategic military risks.

Arms control can and should be an arena for competition in the current security environment. Multilateral and bilateral arms control provides an opportunity for powerful nations to compete openly and fairly in a diplomatic context in ways that can make concrete improvements to security and reduce

strategic risks. Future arms control negotiators will benefit from a more comprehensive understanding of the competitive security environment and the differing perspectives of U.S. competitors on arms control. This understanding could help inform the structures and goals of future arms control arrangements and potential challenges to them.

Arms Control with Peer Competitors

A picture taken in The Hague on June 26, 2018, shows an overview of the opening of an extraordinary session of member states of the Organization for the Prohibition of Chemical Weapons (OPCW).

Photo: Jerry Lampen/AFP via Getty Images

As the security environment has shifted further away from cooperation, the United States, Russia, and China have developed differing and sometimes conflicting strategic perspectives on international security, which will further complicate dynamics in future arms control agreements. For example, on the one hand, bilateral arms control with Russia has not only served as a form of risk reduction but also as a source of status and global leadership for both the United States and Russia. Moscow has long enjoyed the prestige of bilateral "peer-to-peer" arms control agreements with the United States, a feature that continues to animate Russian arms control approaches.[90] At the same time, Russia has consistently violated arms control agreements but resents being treated as a rogue actor and rejects Western claims of a moral high ground. These violations are often motivated by a need to quell dissent and opposition in the international community, preserve vital zones of influence and control, and challenge Western cohesion. In recent years, Russia has grown increasingly dismissive

of multilateral venues and structures such as the OPCW and the Organization for Security and Co-operation in Europe.[91] Nonetheless, Russia seems interested in continued bilateral frameworks that are transactional, quantifiable, legally binding, and interest based.

Russia's poor compliance record with many arms control arrangements—including the INF Treaty, the Presidential Nuclear Initiatives (PNIs), the CWC, and the Open Skies Treaty—underscores the country's rejection of the foundational role that many Western nations assign to rules and the institutions that support and implement arms control. [92] Russia's questionable compliance record raises a potentially major challenge for future arms control agreements: Russia may decide to join international organizations or agreements and test compliance from within rather than not joining an agreement or withdrawing from one in which they know they will be non-compliant. Russia's selective compliance with arms control deals potentially affords it a significant military benefit, such as the development and fielding of prohibited weapons systems.[93]

Unlike the high-level bilateral agreements that characterize the U.S.-Russia arms control relationship, China often prefers multilateral, internationally oriented agreements.[94] In the case of strategic arms control, however, achieving a multilateral deal will be difficult. Most Chinese experts and officials express deep skepticism that U.S. efforts to engage in arms control with China are actually meant to improve strategic stability and limit the risk of nuclear war.[95] Instead, many in the Chinese security establishment believe the United States is attempting to use arms control to lock in its dominant nuclear position, reject mutual vulnerability, undermine China's nuclear deterrent, and win the moral high ground.[96] In 2019, Fu Cong, director-general of arms control at the Chinese Ministry of Foreign Affairs, noted that the global strategic stability architecture was under duress as a result of the collapse or near collapse of arms control agreements. He asserted the United States is attempting to "contain and seek overwhelming military superiority over Russia and China in all fields and with all means imaginable and introducing political ideology into the international discourse on arms control and non-proliferation, leading to heightened risks of an arms race and confrontation."[97]

China's attempts to deflect and avoid bilateral and multilateral arms control efforts will grow increasingly problematic as its nuclear arsenal grows quantitatively and qualitatively. At the same time, incentives to curb arms racing may prove increasingly attractive to Beijing. Most experts agree that arms control efforts with China need to focus less on the numerical aspects of nuclear arsenals and more on the technologically advanced delivery systems that U.S. warning infrastructure may find difficult to detect, along with China's non-nuclear strategic capabilities.[98]

While a trilateral dialogue remains desirable, it may not be realistic given the broad imbalances of capabilities and interests and the insistence from both China and Russia on including France and the United Kingdom in any expanded framework. Integrated arms control, therefore, might explore not only bilateral or trilateral agreements but also broader multilateral risk reduction measures in advanced technologies with both nuclear and conventional applications. Generally, experts agree that without a broader, longer-term dialogue on nuclear risks between the United States and China, it will be difficult to define and scope interests, trade space, and identify risks in ways that facilitate arms control agreements.

Integrated arms control, therefore, might explore not only bilateral or trilateral agreements but also broader multilateral risk reduction measures in advanced technologies with both nuclear and conventional applications.

In addition to addressing rising competition and political challenges, future arms control will need to consider the evolving information environment. Future agreements—and the processes, people, and institutions that support them—will need to develop strategies of resilience to reduce vulnerability to disinformation and digital attack and incorporate the growing role of open-source information and nongovernmental entities in evaluating arms control compliance. Agreements will also need to include guidelines for deconfliction between state- and privately controlled information sources while also leveraging new technologies, especially in the areas of data management and information processing, digital surveillance, and ML, among others. To succeed, arms control must be adapted to these technological and informational factors and the security context and explore alternative structures, modalities, and participation models.

The Role of Partners, Allies, and Existing Institutions

The future of arms control does not solely rest with the United States, Russia, and China. As previously discussed, U.S. allies in Europe and Asia also have a vested interest in future agreements and have launched their own arms control and risk reduction initiatives in recent years. European partners and allies have grown increasingly animated on issues of restoring arms control as a means of managing competition, preventing arms racing, and reducing risks in crises. Going forward, allies and partners' perspectives and inputs will be crucial in order to develop arms control agreements that address the diversity of issues at stake, particularly around the changing security and technological landscapes. Consultations are just the starting point. Allies might also seek to play a third-party role in contributing ideas or facilitating arms control efforts, such as the current work of the German Foreign Ministry. Alternatively, they might highlight potential concerns with arms control agreements that could undermine their security, indirectly shaping the outcomes of agreements. While this is not a particularly new challenge for arms control, it is an increasingly complex one. For the United States, just as integrated deterrence includes integration with partners, integrated arms control must ensure it does not come at the expense of any extended deterrence or assurance commitments and must continue to prioritize allies' security in addition to protection of the U.S. homeland.

Other key stakeholders reside in existing institutions. Differing perceptions of the rules-based international order, including the roles and responsibilities of traditional structures and institutions such as the IAEA, the OPCW, the Conference on Disarmament, or the UN system more generally, will play a role in determining how future arms control agreements are negotiated and what enduring value is assigned to them. Shared interests in these structures and institutions may prompt arms control cooperation, but sovereign interests will ultimately drive the art of the possible with China and Russia. Enduring political challenges and obstructions in

many of these institutions remain a significant challenge to their sustained role in formal arms control agreements. Roles in the competitive playing field will be uncomfortable for arms control institutions and organizations that have grown accustomed to consensus-based decisionmaking, technocratic bureaucracies, and block voting behavior that allowed most participating states to avoid "picking sides" in disputes and conflicts.

Effective dispute mechanisms, a deeper bench of technical expertise in member states, improved cyber defenses and information management systems, and streamlined intelligence sharing will all play important roles going forward. Future arms control agreements will also need to consider a broader scope of capabilities and concerns to account for developing and sustaining agreements under such contested circumstances. Just as important, however, will be issues of scope, as agreements limited to strategic nuclear arms (warheads and delivery systems) will be impacted in different domains and through different technologies, including space, cyber, nonstrategic nuclear, missile defense, emerging chemical and biotech, and advanced conventional weapons systems.

Arms Control Modalities

The arms control landscape is ready for renewal, but that may require exploring and embracing new modalities amid a rapidly evolving strategic and technological environment. In particular, the range of new and existing strategic capabilities suggests the mechanisms and structures of the past, largely involving like-for-like trade-offs or bans on specific capabilities, are unlikely to meet the needs of the emerging security environment. Additionally, advanced technologies that are ubiquitous and dual-use are particularly difficult to define and verify. Verification of nuclear arms control, such as on-site inspections, and legally binding treaties are seemingly at odds with the traits of many emerging technologies that may lack the physical or geographic attributes that made traditional on-site inspections feasible. Ultimately, modalities for integrated arms control will depend on a combination of political, economic, and technological factors. In some instances, this might require designing new agreements tailored to various risks—arms control for cyber, for example, will look very different than arms control for hypersonic missiles. In other instances, new modalities might not even be necessary. Rather, the United States and arms control partners can draw on existing mechanisms and adapt them to new technologies and challenges.

The rich history of nuclear and non-nuclear arms control provides examples of how future agreements might integrate domains, actors, and risks in order to strengthen strategic stability. Factors that ultimately define the nature of arms control agreements can be divided into five separate buckets: (1) precedent; (2) formality; (3) membership; (4) limits; and (5) implementation, verification, and enforcement. How states mix and match elements across these various buckets ultimately depends not only on the behavior of concern and the security environment but also on technological characteristics and how various technologies and domains might interact with each other. Drawing on a broader and more diverse set of tools would allow for greater tailoring and for arms control partners to address a wider range of issues across multiple domains and levels of conflict in developing future agreements. The overall factors present a menu of options for decisionmakers:

Menu of Options for Arms Control

1. Precedent

- Incorporation into preexisting agreements
- Adaptation of preexisting agreements
- Reinterpretation of an existing agreement
- New agreements and modalities

2. Formality

- Legally binding formal treaties
- Formal non-treaty agreements (e.g., executive orders)
- Informal cooperative agreements
- Unilateral measures, (e.g., reductions, transparency measures, or restraint)

3. Membership

- Bilateral agreements
- "P5 process"
- Like-minded states
- Multilateral agreements
- Near-universal participation
- Asymmetric participation (i.e., role of observer states or organizations)

4. Limits

- Reductions to or elimination of specific classes of weapons or capabilities
- Reporting or notification requirements
- Behavioral constraints
- Asymmetry of domains, reductions, and ceilings
- "Catch-all" language
- Risk reduction measures (e.g., crisis communication channels)

5. Implementation, Verification, and Enforcement

- Monitoring and inspections (e.g., remote, on-site, automated, or in person)
- Dispute resolution mechanisms (e.g., consultative bodies, investigative mechanisms, challenge inspections)
- Expanded mandates for existing international organizations (e.g., OPCW, CTBTO, IAEA)
- National implementation and regulation (e.g., model legislation efforts)
- Preemptive notifications (e.g., Outer Space Treaty)

PRECEDENT

Arms control agreements do not necessarily start with a completely blank slate. For most of today's challenges, there are arms control precedents and prior or preexisting agreements that offer valuable starting points. In some areas, however, the geopolitical and technological landscape may require entirely new arms control modalities. And yet, even here, existing precedents can point in new and constructive directions. Managing risks associated with AI, for example, seemingly falls outside the purview of any existing agreements. Arms control for AI would face a host of unique verification and transparency challenges entirely distinct from historical arms control efforts, such as limits of nuclear delivery vehicles (which can be counted through inspection) or biological weapons (which are regulated through domestic legislation). But existing arms control agreements might offer solutions for some emerging technologies and should be utilized where possible. Hypersonic glide vehicles, for example, are arguably covered by New START, despite not being listed explicitly in the treaty protocol. While New START is a relatively discrete and specific arms control agreement, others could provide more flexibility, adaptability, and resilience to take on advanced technologies.

Preexisting agreements can either incorporate new capabilities or be amended to expand their remit. For example, the Hague Code of Conduct, Vienna Document, and crisis hotlines are existing arms control and risk reduction measures that could potentially be expanded to support further risk reduction efforts. The P5 process, for instance, might offer a unique opportunity for gradually exploring arms control and risk reduction measures without negotiating an entirely new agreement. This might also entice Chinese engagement in arms control because China attaches "great importance" to their work in the P5 process.[99] A slightly more ambitious option would be to expand the mandate of existing agreements and institutions. For example, in the context of the P5 process, the group has historically taken on new issues such as transparency of doctrines and strategic risk reduction. In some instances, of course, forums for dialogue and cooperation might not exist and therefore would require developing an entirely new agreement.

FORMALITY

Another factor in designing integrated arms control is the formality of an agreement. Treaties offer a highly formal and codified form of cooperation, entrenching states within international law and (typically) requiring domestic legislative approval, such as advice and consent from the U.S. Senate. While generally more durable and resilient to political and policy shifts, treaties are often slow to negotiate, even slower to ratify, and almost impossible to amend, which presents a challenge for many technologies that are evolving at a rapid pace. In addition to treaties, states might consider less stringent and more informal means of codifying cooperation, although these are more susceptible to political shifts with less built-in resilience. Sarah Kreps has suggested "international negotiators might be better served drafting less highly legalized agreements that offer latitude in states' commitment to the agreement, since the prospect of tying their hands will discourage states from engaging in higher-obligation commitments."[100]

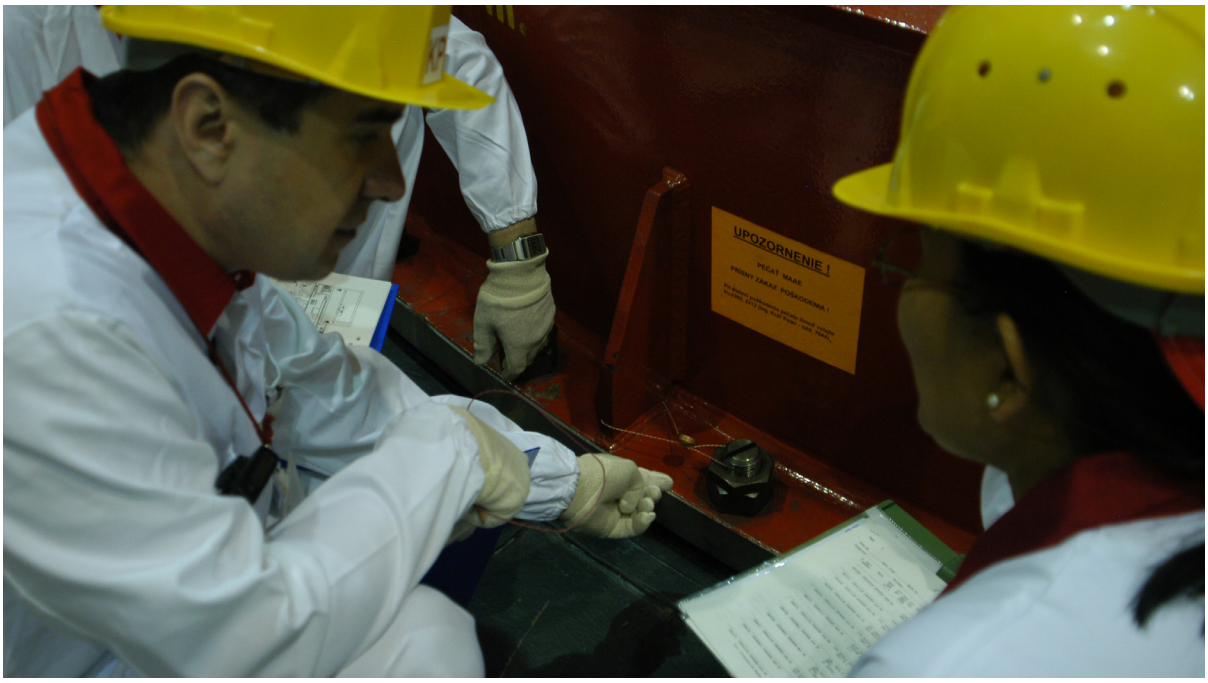
The Joint Comprehensive Plan of Action (JCPOA) is one example of an arms control agreement without a treaty. But other informal agreements might include cooperative risk reduction efforts, such as the Hague Code of Conduct, whereby states voluntarily commit to various transparency and predictability measures. Other efforts might include agreements for information exchanges. For example, in the context of future U.S.-Russia arms control, Vince Manzo offers options for transparency and restraint without a treaty, such as pre-notification schemes "to augment U.S. and Russian efforts to independently

verify information they receive through the data exchanges and improve confidence in their assessments of the other's deployed nuclear forces."[101] These less formal options might allow for cross-domain or non-like-for-like exchanges whereby states have flexibility in how they design their own force postures. An even more informal option would be unilateral measures, such as the Presidential Nuclear Initiatives or commitments to unilateral restraint.

MEMBERSHIP

The third consideration for arms control modalities is the scope of membership. At one end of the spectrum of options are near-universal agreements, such as the CWC and the Nuclear Non-Proliferation Treaty (NPT); at the other end are bilateral strategic treaties, such as New START. Some agreements include a diverse mix of states with differing roles, such as the NPT, which includes possessors and non-possessors. Others include only like-minded states, such as the TPNW, which is an attempt by a group of nuclear non-possessors to develop a norm to impact possessors. Again, this points to a range of possibilities for future arms control agreements that might exclusively include possessors of technologies, such as AI-enabled conventional weapons, or a more wide-ranging agreement, such as through the UN Group of Governmental Experts process. To account for new stakes and new stakeholders, flexibility in membership and exploring a wider range of arms control institutions will be crucial.

For more multilateral agreements, there is also the question of who decides on membership. Is it open to any states or are there pre-membership requirements? And how do states exit an agreement? This will largely depend on the formality and legality of an agreement. States might choose to design relatively open and flexible agreements allowing for anyone to join, as with participation in UN initiatives such as



An IAEA safeguard inpector checks one of the IAEA seals deployed in one of the reactor units at the Mochovce Nuclear Power Plant (NPP) on January 18, 2005.

Photo: Dean Calma/IAEA

Open-Ended Working Groups. Alternatively, agreements such as the NPT require states to meet certain requirements prior to membership, namely relinquishing any nuclear ambitions for the non-nuclear weapons states.

LIMITS

In the context of arms control, "limits" refer to the terms or constraints of an agreement itself—this might include reductions in existing capabilities, capping current levels for certain types of weaponry, prohibitions on certain actions or behaviors, or elaborating new confidence-building measures. Many emerging strategic risks include military capabilities powered by technologies that are either new or privately owned, and states are therefore reluctant (or unable) to reduce or limit their development. There have been numerous efforts to develop best practices, such as the Tallinn Manual for cyber, or to increase transparency, such as discussions in the P5 process on doctrines. These efforts have the potential to lay the groundwork for arms control agreements but have not yet been realized. Agreements such as the CWC encompass a wide range of limits, as they both restrict certain categories of weapons and are highly specific while also including broad "catch-all" language.

Traditional quantitative limits would be challenging for many advanced technologies, so agreements instead might have to focus on constraining activities, or behaviors, rather than technically defined capabilities. In other areas, such as space-based technologies or deep undersea capabilities, inspection-based protocols are unrealistic. The establishment of a UN Open-Ended Working Group to address the security threats of kinetic anti-satellite weapons could be a step in the direction of space arms control.[102] Another example that might be particularly useful for cyber activities is a twenty-first-century version of the Incidents at Sea Agreement, which did not reduce any capabilities or impose any limits but rather required states to abide by a certain code of conduct and engage in transparency and confidence-building measures, particularly during crises. Conversely, while many technologies such as advanced biotech and biochemical engineering, 3-D printing, and AI-enabled autonomous systems can have high-risk military applications or pose potential dangers involved in their misuse or proliferation, these capabilities have profoundly important civilian applications that should not be curtailed or limited.

But limits also include the duration of an agreement as well as when and how it will come to an end. While treaties such as New START include an optional extension clause, exercising an extension often becomes a politically charged exercise and can increase pressure on the agreement itself. Conversely, the INF Treaty did not have an end date beyond the final inspections of the removal of INF systems. But agreements with indefinite durations struggle, as they may not be flexible enough to adapt to a changing strategic landscape or technological advances. More regularized opportunities to adapt and amend agreements may be increasingly important in new and complex arenas where both the technologies and their potential military applications are rapidly evolving.

IMPLEMENTATION, VERIFICATION, AND ENFORCEMENT

Implementation can entail a host of activities, including reporting, monitoring, conflict resolution, verification, and enforcement, all of which can be tailored as required to accommodate security considerations in a multidomain environment. Implementation typically entails technical or operational activities to gather information and evidence about parties' adherence to an agreement's provisions. Dual-use technologies are notoriously hard to monitor, not only because of their use in the civilian sector but also because of the role of the private sector and concerns about proprietary

information and intellectual property. For this reason, the BWC, as one example, lacks a robust verification mechanism, thereby avoiding dual-use challenges altogether.

Other arms control agreements, however, such as the CWC, tackle dual-use technology in a variety of ways, including highly specific schedules of militarily relevant chemical agents and processes, domestic regulation, on-site inspections, and challenge inspections. Another example is a multitool approach to verification, such as the monitoring and verification of biological and chemical weapons in Iraq following the Gulf War, which was developed through the UN Security Council and includes monitoring of imports and exports along with on-site inspections to facilities.[103]

And yet another approach is for states to be individually responsible for verification, such as the Land Mines Convention, which states:

> Each State Party shall make every effort to identify all areas under its jurisdiction or in which anti-personnel mines are known or emplaced and shall ensure as soon as able that all anti-personnel mines in mined areas under its jurisdiction or control are perimeter-marked, monitored, and protected by fencing or other means, to ensure the effective exclusion of civilians until all anti-personnel mines contained therein have been destroyed.[104]

Relying on domestic regulation may be particularly valuable for agreements on biotech, AI, or other dual-use technologies that are largely being developed by the private sector. Other nonproliferation mechanisms, such as UNSCR 1540, have emphasized the importance of strong domestic or national legal and regulatory systems to enforce international commitments. Model legislation proposals have also been helpful in the past to implement stronger domestic enforcement mechanisms. Moreover, traditional inspections are but one option for verification. Persistent challenges include warhead verification, remote monitoring, and protection of national security information. Increasingly, arms control efforts must seek to address risky behaviors and new technologies where technical verification of compliance could be very challenging. Despite these difficulties, dramatic improvements in remote sensing, persistent electronic surveillance, big data management, and other potential monitoring techniques may open new verification pathways. This might include inspections, sampling, data exchanges, declarations, and open-source-based remote-monitoring approaches that are not necessarily state controlled. AI and open-source analysis might contribute to arms control verification through pattern recognition and object identification.[105] The use of AI-enhanced monitoring would force states to go to greater lengths to hide cheating and might also reduce the need for on-site inspections.[106] Additionally, new digital information technologies could provide a pathway for less-intrusive verification. Most arms control agreements will entail a combination of these activities to improve confidence in agreement compliance. Emerging technology and innovation for monitoring and verification have been a primary area of emphasis. The International Partnership for Nuclear Disarmament Verification (IPNDV) is one such example. Begun in 2014 and led by the U.S. Department of State in cooperation with the Nuclear Threat Initiative, IPNDV is composed of more than 25 countries with and without nuclear weapons that identify challenges associated with nuclear disarmament verification in order to develop potential procedures and technologies to address the challenges.[107]

In addition to verification options—from on-site inspections to a multitool approach—arms control agreements have included a range of compliance and enforcement mechanisms that improve transparency and encourage parties to an agreement to share concerns, report technical noncompliance, and work to preserve and enforce agreements through cooperative measures and

dialogue. Some violations are genuinely accidental. Others are militarily significant. Agreements might include consultative committees or other dispute resolution bodies to address discrepancies and support technical dialogue and problem solving. Ultimately, compliance is a political activity, in contrast to technical activities such as verification, and disputes will inevitably arise. Mechanisms that allow parties to address and reconcile any disparities that arise will help to provide a forum for competition and conflict in arms control without necessarily derailing such agreements altogether. One approach to compliance is consultations prior to deployment to determine whether or not an activity would undermine the agreement. Such an approach was employed by the Outer Space Treaty, which required states to "undertake appropriate international consultations before proceeding with any such activity or experiment."[108]

Across each of these categories—precedent, formality, membership, limits, and implementation, verification, and enforcement—there is a spectrum of options for arms control agreements. This might include familiar options, such as using existing agreements or pursuing bilateral strategic treaties similar to the Cold War. It might also include exploring a wider range of arms control tools beyond bilateral nuclear treaties, such as broader risk reduction agreements or mechanisms in non-nuclear treaties, such as the BWC and CWC. Integrated arms control can draw on a variety of these tools to improve security in this complex and multidomain environment. There is unlikely to be one single agreement to address concerns about Russia, China, and other actors, or to capture all the capabilities and advanced technologies that could come into play in a crisis. Instead, the United States can use the rich history and menu of options to tailor arms control as necessary. Ultimately, arms control is a political exercise, and how states draw from the menu of options will ultimately be determined by what states hope to achieve from an agreement.

6

Conclusions and Recommendations

Realizing an Integrated Arms Control Strategy

While broader goals of disarmament may be desirable, the most pressing objective for arms control in the current security environment must be the prevention of major war, especially war that would occur under a dangerous nuclear shadow, risking catastrophic escalation in the event of deterrence failure. At the same time, arms control might be harder to achieve today due to a series of factors and trends in the international security environment including the decline in trust between the United States and potential arms control partners; the rise in complex, highly interrelated, strategic technologies; the emergence of a highly digitized, privately controlled, and easily weaponized information environment; and the presence of increasingly assertive regional stakeholders.

Moreover, technological trends suggest that rather than seeking to impose numerical constraints on specific technologies, states might prioritize arms control efforts that target specific behaviors of concern, regardless of the technological capabilities involved, and explore a wide range of arms control modalities to reduce the risks of arms racing and improve crisis stability. As a result, successful arms control tools must be adapted to account for these challenges and should consider alternative structures, modalities, and participation models.

Furthermore, as deterrence becomes more integrated across diverse technologies, domains, risks, and actors, so too must arms control. Deterrence alone may struggle to deal with these emerging escalation dynamics, and arms control has the potential to contribute by managing capabilities and technologies across domains and levels of competition and conflict. Arms control and related risk reduction measures can mitigate escalatory pressures, such as with multilateral crisis communication channels. Now is the time for a recoupling of arms control with deterrence in a way that recognizes these new realities.

Given that arms control and deterrence go hand in hand, a successful integrated deterrence strategy demands similarly integrated and cross-domain arms control approaches. Arms control efforts must rise to a similar level of ambition in terms of integration, flexibility, and creativity, including in areas of hybrid or gray zone competition, where interests are increasingly challenged and escalatory risks poorly understood. Such a strategy should set clear objectives and priorities, identify structures and modalities that improve resiliency and reinforce stability across the spectrum of deterrence challenges, and guide the organizational, resourcing, and structural reforms necessary to implement such a strategy successfully.

Integrated arms control should be based on three broad principles: enhancing stability, embracing plurality, and reinforcing resiliency. First, arms control remains a powerful tool for strategic stability and managing risks associated with crisis escalation and arms racing. This can and should work hand in hand with deterrence, and integrated arms control should be incorporated into any integrated deterrence strategy. Second, arms control will need to be flexible and operate across a plurality of technologies and actors. Integrated arms control must be multidomain, multilateral, and agile. Amid geopolitical and technological changes, strategic stability is becoming increasingly complex and will require a more flexible approach to arms control than is typically provided by legally binding bilateral agreements that focus on single technologies or domains. At the same time, these integrated approaches will require partners and allies across the international landscape that are more capable, engaged, and empowered. Finally, an effective integrated arms control strategy will require that the United States organize and invest to create the structural, technical, and operational capabilities necessary to support such an approach in ways that are durable and sustainable.

Enhancing Stability

- **Recognize arms control as a constructive forum and outlet for strategic competition.** Nuclear arsenals are expanding both quantitatively and qualitatively, accompanied by a broader set of strategic delivery systems and high-impact technologies, which will challenge existing U.S. defensive systems. Meanwhile gray zone activities will further complicate concepts of escalation. Arms control can offer the United States, China, and Russia an opportunity to compete openly and fairly in a diplomatic forum that reduces risk and encourages stability.
- **Prioritize efforts that mitigate escalatory pressures that raise the risk of major war between nuclear-armed states**. While broader goals of disarmament may be desirable, the most pressing objectives for arms control in the current security environment must be preventing major war and reducing the risk of catastrophic escalation in the event of deterrence failure.
- **Address a range of stability challenges across multiple domains and technology types.** Nuclear arms control, such as a follow-on agreement to New START, remains critically important. However, it should not be prioritized to the exclusion of other arms control and risk reduction efforts in other arenas, such as biotechnology, advanced missile threats, space, cyber, and digital technologies, in which stability risks, both in terms of crisis management and arms racing, are of growing concern.
- **Focus on particularly risky behaviors, especially the application of advanced technologies during crisis scenarios.** Arms control arrangements that focus on banning or limiting specific

numbers and types of weapons will continue to play a role in strategic stability, especially in terms of nuclear weapons and related delivery systems. But the intersection of nuclear and advanced technologies, especially during crises with compressed decisionmaking time, will also need to be a priority. Such agreements could address behaviors across the range of conflict that might erode or destabilize an integrated deterrence framework. Some specific priority areas for integrated arms control and risk reduction efforts that might address these behaviors include:

Decision Interference: Effective crisis management demands that national decisionmakers retain the ability to communicate with their citizenry while also controlling military forces without interruption. Actions that deprive leaders of this ability pose substantial risks, whether through deep fakes, cyberattacks that disrupt national communication infrastructure, or direct attacks on space-based assets essential for strategic command and control, pose particularly severe stability challenges. These risks suggest that arms control approaches should focus on fail-safe decisionmaking, such as reciprocal agreements to prohibit digital identify manipulation of national decisionmakers and others within the nuclear chain of command, or establishment of cyber or space-based "no go" zones designed to support risk reduction.

Predictive Surveillance: Warning is essential for stable deterrence, providing essential decision time necessary to authenticate hostile action, assess for accidents and errors, and consider alternative courses of action. Dramatic improvements in remote sensing, data processing, and ML combined with new remote sensing platforms such as AI-enabled drone swarms and LEO, small satellite constellations, will potentially transform strategic warning systems as military leaders seek information superiority in decision-support architectures. Such capabilities can potentially reduce miscalculation risks, but they can also erode the opacity that protects second strike forces, while driving up incentives for conventional, and perhaps even nuclear, first strike. Moreover, the technological drive for decision dominance and information superiority could open new doors for anticipating adversary actions and encouraging preventive military action. Arms control and confidence-building measures focused on protected opacity, shared warning data, strategic military deconfliction mechanisms, and notification requirements may help to ameliorate the downside risks associated with these new systems and capabilities.

Autonomous Strike: Accelerated and autonomous strategic strike systems, even at the conventional level could fuel first-strike incentives and exacerbate arms racing. Person-in-the-loop requirements can provide assurances and clarify normative standards even if verification and enforcement will prove challenging. There also may be ways to build AI-enabled "fail-safe" capabilities that improve nuclear weapons security, ensure continuous positive control, and better detect warning errors. Much like systems and principles for warhead security, such technologies might even be developed and distributed through cooperative approaches with other nuclear armed states.

Conventional Firebreaks: Faced with eroding strategic-level firebreaks, integrated deterrence approaches that prioritize preventing major warfare between major nuclear armed powers will require renewed focus on conventional arms control that seeks

to contain and manage crises at lower focus echelons of conflict. In particular, close-proximity approach operations among space, air, and sea-based assets can easily escalate when forces or assets come into contact. Multilateral agreements to curtail risky behaviors in space, including debris-generating events and high-risk approach operations would reduce both deliberate and inadvertent stability risks in this high-consequence domain. Declared surveillance activities, separation of forces and assets agreements that might reinforce guard rails around tripwire capabilities, and limits on the size, duration, and intensity of military exercises in border regions all could play a role in reducing conventional escalation risks. Similarly, establishing payload limitations on high-maneuverability, intermediate, and long-distance strike platforms could reinforce clearer conventional/nuclear firebreaks even as verification challenges would remain considerable.

Embracing Plurality

- **Expand cross-domain, non-like-for-like approaches in future agreements.** With advanced technologies and cross-domain challenges, strategic stability may be better reinforced through arms control efforts that utilize cross-domain, mixed technology trade space. This concept of asymmetric arms control can facilitate more creative ideas for agreements across actors and domains.[109] Such agreements might include the exchange of non-like-for-like capabilities, or it might entail a broad overarching agreement that allows states to structure their forces asymmetrically within the terms of the agreement.
- **Incorporate new technologies, such as gene editing or offensive cyberattacks, into existing agreements, specifically in military contexts.** For example, military applications of CRISPR DNA and other forms of genome editing might be addressed through the BWC.
- **Prioritize allies, partners, and other essential stakeholders' perspectives in pursuing integrated arms control.** Going forward, allies and partners' perspectives and inputs will be crucial to develop arms control agreements that address the diversity of issues involved and the asymmetry of stakes among various participants. In some instances, allies and partners might be amenable to being more formally involved in existing agreements, particularly those focused on risk reduction, as occurred in the CEND initiative. More ambitious involvement might include participation in consultative and ad hoc advisory bodies or affiliation with existing and new mechanisms, especially those that improve resiliency and address regional security concerns. Ultimately, however, this will depend on allies and partners' priorities and interests, in consultation with the United States.
- **Support stronger capacity-building efforts among allies and partners to improve technical capacities for arms control.** That will include verification, monitoring, investigations, forensics, and attribution efforts as well as sharing expertise and technical knowledge in these areas. Cooperative threat-reduction programs at the Departments of Defense and State bring considerable expertise and experience in these areas that could be adapted to the needs of an integrated arms control strategy.
- **Create positive incentives for multilateral cooperation in risk reduction efforts.** In areas of dual-use technologies—such as AI, biotechnology, and chemical engineering—arms control partners can focus on agreements that offer more "carrots" rather than "sticks," such as access to shared technology, preferred trade and market access, and technical capacity building, especially in areas such as threat detection, investigations, forensics, and emergency response. Risk reduction efforts

Delegations from the UN Security Council's five permanent members (P5), China, France, Russia, Britain and the United States, attend a Treaty on the Non-Proliferation of Nuclear Weapons (NPT) conference in Beijing on January 30, 2019.

Photo: Thomas Peter/AFP via Getty Images

could be particularly valuable in promoting safe science initiatives to regulate dramatic advances in technology, such as codes of conduct among scientific communities to preserve benefits while mitigating security risks and to enhance multilateral oversight of dual-use research of concern.

- **Catalogue existing risk reduction and stability promoting tools through multilateral forums, such as the P5 process.** Integrated arms control will not necessarily require inventing new structures or tools. Indeed, numerous mechanisms already exist to promote strategic stability, particularly crisis stability, such as hotline agreements. Many of these, however, are underutilized or less well known. As part of their work on strategic risk reduction, the P5 process or the CEND initiative, in partnership with nongovernmental experts, should catalogue existing mechanisms for risk reduction. This could include efforts such as identifying and disclosing existing hotline mechanisms, encouraging sharing of such mechanisms across the P5, broadening membership and reach of the Nuclear Risk Reduction Center network, and pursuing multilateral crisis communications, such as through CATALINK, a collaborative "hotline" project led by the Institute for Security and Technology.[110]

Reinforcing Resiliency

- **Emphasize dispute resolution mechanisms.** This might include expanding compliance-reporting pathways and investigatory procedures, cooperative consultative processes, and other mechanisms. These mechanisms might accompany robust verification activities, such as on-site inspections, or could be part of more informal agreements that might not have intrusive verification beyond NTM. Indeed, as AI, open-source analysis, and other digital verification tools become more advanced, they could increase the amount of enforcement and compliance data that will require clarification and forums for dialogue.

- **Increase investment in research and development of arms control technologies designed to improve remote monitoring, enhance technical verification, better detect violations, and improve confidence in technical compliance while reducing intrusive requirements.** The Defense Threat Reduction Agency and the national laboratories are well equipped to focus on the technical requirements of integrated arms control and to create the implementation technologies necessary to be effective and enforceable.
- **Expand the cadre of qualified U.S. operational, technical, and policy personnel capable of supporting integrated arms control efforts.** Integrated deterrence as a military strategy will be implemented through a vast network of military planners, operators, and resource managers at the military services and combatant commands as well as policy professionals and the Joint Staff. Comparatively, the interagency human capital devoted to integrated arms control is vastly under-resourced at a time when arms control "multitasking" will be needed to engage across a diverse set of security imperatives.
- **Formalize and professionalize the role and development of open-source monitoring and verification in arms control agreements and institutions.** The United States should encourage collaborative efforts through private entities and international institutions to create codes of conduct, peer review processes, and standards of evidence for open-source analysis. This will especially require supporting the development and professionalization of open-source verification, monitoring, and analysis, while simultaneously maintaining clear separations from proprietary government sources of information such as intelligence and NTM.
- **Establish information security as a fundamental component of arms control, from negotiation to implementation.** Comprehensive, end-to-end information security practices to combat disinformation and influence operations should be built into all stages of the arms control process. Future agreements will be negotiated and implemented in a complex, technology-driven, and easily weaponized digital information ecosystem. Information security practices will be essential to counter the influence operations and other digital information risks that will be a feature of future arms control from negotiation to implementation and compliance.

Appendix A

Canary in the Coal Mine:

The Chemical Weapons Case Study

The chemical weapons arena provides an interesting case study for arms control in an era of competition, as the use of disinformation as a "fog-of-war machine" to shape rhetoric and public opinion on arms control has never been more apparent. Furthermore, leading open-source investigations and organizations have been borne out of this arena and provide an example of how such capabilities could be leveraged for verification and compliance. At the same time, the Chemical Weapons Convention (CWC) has avoided complete collapse, despite noncompliance by states party to the agreement and disagreements within the Organisation for the Prohibition of Chemical Weapons (OPCW). This "canary in a coal mine" case study could lead to a better understanding of the challenges and opportunities for verification and compliance in the evolving information ecosystem as well as a more flexible structure for arms control agreements.

The intentions behind the use of disinformation surrounding the more than 336 recorded chemical weapons attacks are clear: deny the occurrence of events, misidentify victims and targets, discredit and falsify motives and identities of witnesses and responders, and elevate "authority" figures who seek to promulgate counternarratives.[111] Through these actions, perpetrators and their allies seek to assure that attribution and accountability for the violation of international norms and laws cannot be established, noncompliance in international agreements cannot be determined, and both political and military international intervention is discredited or prevented.

In the wake of the April 7, 2018, chemical weapons attack in Douma, Syria, a widespread disinformation campaign ensued, first attempting to deny the occurrence of the attack and then trying to discredit the findings of the OPCW. Immediately following the attack, Syria and Russia launched a large-scale, persistent disinformation campaign through official Twitter accounts and state-backed media outlets.[112] The largely state-directed information operation attempted to flood the zone with

conflicting and contradictory theories and narratives, alternating between outright denials and false-flag claims. Initially, the campaign had little impact, as the space was dominated by mainstream media coverage of the attack and the international response. However, as the media turned to other news stories in the following week, disinformation took over.

As mainstream media attention shifted away from the attack, the disinformation campaigns continued, but with much more success. From April 10 to 16, 2018, "six of the ten most-retweeted posts [on the topic] came from Assad supporters, out of a total 487,000 posts," indicating that the pro-Assad voices were dominating the conversation on Douma.[113] A study by Jack Nassetta and Ethan Fecht found a network of synthetic actors (e.g., trolls, bots, and cyborgs) was activated in the days following the attack. The synthetic accounts attempted to defame Western institutions to discredit claims of Syrian chemical weapons use, suggest jihadist responsibility for the attacks, hint that destructive (specifically through nuclear means) escalation would result from a Western retaliatory strike, and prey on Western religious and cultural sympathies.[114] During the same timeframe, a Russian GRU cyber intelligence warfare team attempted to hack into the OPCW but was ultimately foiled by the Dutch government.[115]

As the disinformation spread on social media platforms, the state-directed disinformation campaign morphed into a more complex and hybridized campaign, linking and leveraging online activists.[116] The counternarratives on Douma quickly moved beyond fake and propaganda websites with manipulated journalistic content to rapidly spread through a network of online activists and "independent" journalists. These individuals came from both far left and far right perspectives and had strong track records of opposing U.S. and UK foreign policy, "interventionist" policies, and international institutions.

Douma also offers an interesting case study for disinformation-shaping rhetoric due to a series of information "leaks" from "whistleblowers" at the OPCW, following the publication of official findings. The leaks and whistleblowers, who disputed the OPCW's official findings confirming the occurrence of a chemical weapons attack, were subject to an independent investigation, which concluded the "whistleblowers" misrepresented their connections to the OPCW and the Douma investigations team and committed a serious deliberate and premeditated breach of confidentiality.[117] The OPCW supported the published official findings, but the damage was done. Now, not only were Western states—the United States, the United Kingdom, and France—under attack, but so were the international institutions. This affected the discourse within more fringe online activist communities but increasingly included politicians and other more mainstream influencers as well, such as then-2020 presidential candidate Tulsi Gabbard and actress Susan Sarandon, who retweeted Douma-related disinformation to her 680,800 followers, proving reputable voices can become enablers of these false and misleading narratives, whether wittingly or not.[118]

Following the chemical weapons attack in Douma and the use of chemical weapons against the Skripals in the United Kingdom, the OPCW established the Investigation and Identification Team (IIT) in June 2018 as an attribution mechanism to identify perpetrators and enablers of chemical weapons use in Syria based on incidents of use identified by the Fact-Finding Mission or not previously reported by the Joint UN-OPCW Investigative Mechanism.[119] To date, the IIT has identified nine cases in Syria to investigate and released two reports that, under reasonable grounds, identify the Syrian air force as the perpetrator of chemical weapons use in Latamneh in March 2017 and Saraqib in February

2018.[120] Following the publication of the second report in April 2021, the Conference of States Parties to the CWC adopted a decision to "suspend certain rights and privileges of the Syrian Arab Republic under the Convention pursuant to paragraph 2 of Article XII of the Convention."[121] These rights and privileges include voting in the Conference and the Executive Council, standing for election to the Executive Council, and holding any office of the Conference, the Executive Council, or any subsidiary organizations.[122] The decision passed with 87 states voting in favor, 34 abstaining, and 15—including Russia, China, Iran, and Syria—opposing.[123]

As mentioned in the report, the OPCW and CWC have been further challenged by the poisoning of Russian political dissenter Alexei Navalny with a Novichok agent in 2020 and Russia's subsequent response. In October and November 2021, 45 CWC states parties requested that Russia "clarify and resolve" unanswered questions regarding Russia's handling of the Navalny poisoning.[124] Russia responded by accusing the questioning parties, mainly Germany, France, and Sweden, of staging the evidence and of acting unjustly.[125]

In the open-source realm, Bellingcat proved the advantage of open-source research by producing a detailed investigation of the Douma attack just four days later. The investigation used photos, videos, and graphics to conclude that it was highly likely that a gas cylinder, likely containing chlorine gas, was dropped from a helicopter originating from a Syrian air base.[126] Bellingcat's investigations into the attack continued to dispute Russia and Syria's false-flag claims while the OPCW conducted its official investigation. The OPCW interim report was published in July 2018, three months after the attack and Bellingcat's findings, with the final report not published until March 2019, almost a year after the attack.[127] Bellingcat's report was met with a fair share of criticism and skepticism by so-called experts, such as Ted Postol, media outlets, and other open-source intelligence (OSINT) organizations claiming the munitions were staged and therefore an attack did not occur. The claims of a staged attack further escalated with the OPCW "whistleblower" leaks. In response, Bellingcat published a four-part series examining and debunking the OPCW leaks to confirm the official findings, but the rhetoric and conspiracy theories were already in mainstream media.[128] For its efforts, Bellingcat has become involved with the International Criminal Court's Technology Advisory Board and has also received interest from the International, Independent and Impartial Mechanism (IIIM) on Syria, showing the role open-source investigation can play.[129] Bellingcat also published a series of investigations on the Navalny poisoning.

Implications

As the information ecosystem continues to evolve, it is hard not to expect adversaries to leverage the space to conceal non-compliance and cheating, but with the advancement of cyber capabilities, adversaries could also steal information on other parties. Furthermore, advanced capabilities such as deepfakes and AI could be used to create knowledge gaps through automated deception. Future agreements will need to inoculate organizations responsible for verification and compliance against disinformation as well as harden it against cyberattacks and spoofing.

The case of Douma shows that sustained disinformation campaigns, aided by social media, can be successful in distorting the events and allowing perpetrators to get away with violations. However, the case study of Douma also shows how open-source investigations can be leveraged by the international community for verification and compliance in future arms control agreements. The

work by Bellingcat and other open-source organizations produced timely research that backed OPCW findings and debunked the false claims of the "whistleblowers." Going forward, credible open-source investigations of compliance could supplement NTM by providing publicly available information on compliance and verification.

In addition to providing insight into how the nuclear arms control arena could be affected by the challenges and opportunities of the evolving information ecosystem, the chemical arms control arena offers perspective on the structure and modality of future agreements. The reemergence of chemical weapons use, albeit in smaller-scale scenarios, by states party to the CWC underscores the changing threat environment and just how difficult it can be to adapt existing instruments to new threat environments. While the United Nations and the OPCW have created mechanisms to investigate and attribute chemical weapons use, little has been done to enforce obligations to the CWC and hold perpetrators accountable. Moreover, there is a collapse of consensus within the OPCW Executive Council as a result of the more contentious diplomacy measures taken. Future arms control agreements of all types will need to weave in measures to sustain the agreement while also allowing latitude to adapt to new security realities. Furthermore, fully implementing all aspects of agreements is important to both the existing agreements and to measure the success of future agreements.

Appendix B

Disinformation and Covid-19 Case Study

The Covid-19 pandemic highlighted the challenge of disinformation and verification. Following the global spread of the virus, China, Russia, and Iran began disinformation campaigns to sow doubts about the origins of Covid-19.[130] Initial disinformation about Covid-19 was primarily spread through Twitter, with 200 Chinese diplomatic and state-run media accounts pushing out 90,000 tweets between April and May 2020. The tweets are typically in English or Mandarin, though tweets from diplomatic accounts are often in the language of the embassy's host country.[131] Russia and China amplified disinformation on Twitter to play into existing conspiracy theories and promoted the findings of so-called influencers.[132] The use of information laundering, or the process by which disinformation is legitimized through intermediate networks to obscure the original source, allowed for the same disinformation to be spread at a rapid rate throughout different countries.[133]

The speed at which disinformation could spread on social media is exemplified by the success of the Plandemic "documentary," a 26-minute-long video that claims that Covid-19 is the result of a group of shadow elites using the virus and potential vaccine to profit and gain power.[134] The video was posted May 4, 2020, on Facebook, YouTube, Vimeo, and a host website and quickly gained traction on a QAnon-dedicated Facebook group and among anti-vaccine proponents. In just over a week, the video had over 8 million views across a host of platforms and generated countless other posts speculating about the origins of the virus.[135]

Implications

The controversy surrounding the origins of the Covid-19 pandemic, whether natural or gain of function research, has led to questions of China's adherence to the Biological Weapons Convention

(BWC) and has created a greater sense of urgency for creating verifiable and enforceable arms control agreements. The existing BWC framework has limited verification and enforcement measures, and the Covid-19 pandemic highlighted the difficulty in regulating and controlling high-risk biotechnologies and pathogens. And while it is likely impossible at this point to adjudicate the origins of the virus, it may be possible to explore measures to regulate disinformation in future arms control agreements. Although the World Health Organization's proposed "pandemic treaty" does not actively address disinformation, it aims to improve accountability and shared responsibility, transparency, and cooperation within the international system's rules and norms through a series of incentives as well as sanctions or punitive measures.[136] Furthermore, a recent push from the EU Council to align public messaging efforts during future pandemics could be another way to help address information operations. Finally, the Covid-19 pandemic could make the argument for the creation of a new arms control agreement on biological weapons that manages or limits gain of function research, detects risky behavior, and does not just adjudicate blame after the fact but works to regulate responses during a crisis.

About the Authors

Rebecca K.C. Hersman is director of the Project on Nuclear Issues and senior adviser with the International Security Program at the Center for Strategic and International Studies (CSIS). A leading expert on nuclear, chemical, and biological weapons policy; global health security; and crisis management, Ms. Hersman leads the preeminent national program designed to develop next-generation nuclear expertise. An author of numerous studies and reports on nuclear and chemical weapons policy, emerging technologies and strategic stability, and crisis management and decisionmaking, Ms. Hersman also cochairs the CSIS U.S./UK/France Trilateral Dialogues on Nuclear Issues and has served as a commissioner on the CSIS Commission on Strengthening America's Health Security. Ms. Hersman joined CSIS in April 2015 from the Department of Defense (DOD), where she served as deputy assistant secretary of defense for countering weapons of mass destruction since 2009. In this capacity, she led DOD policy and strategy to prevent WMD proliferation and use, reduce and eliminate WMD risks, and respond to WMD dangers. She was a key leader on issues such as the elimination of Syria's chemical weapons, nuclear response and mitigation during the Fukushima crisis, and WMD interdiction policy and response. Ms. Hersman led DOD engagements on WMD issues with NATO, South Korea, Japan, and others, and also served as DOD's principal policy advocate on WMD arms control, nonproliferation, and threat reduction. Prior to joining DOD, Ms. Hersman was a senior research fellow with the Center for the Study of Weapons of Mass Destruction at the National Defense University from 1998 to 2009. Ms. Hersman previously held positions as an international affairs fellow at the Council on Foreign Relations, a special assistant to the undersecretary of defense for policy, and a member of the House Armed Services Committee professional staff. She holds an MA in Arab studies from Georgetown University and a BA from Duke University.

Heather Williams is a visiting fellow with the Project on Managing the Atom at Harvard Kennedy School. She is visiting from King's College London where she is a senior lecturer (associate professor) in the Defence Studies Department and Centre for Science and Security Studies. From 2020 to 2021 she was a Stanton Nuclear Security fellow at the Massachusetts Institute of Technology (MIT), and from 2018 to 2019 she was a specialist adviser to the House of Lords International Relations and Defence Committee. Her research focuses on arms control, emerging technologies, crisis escalation, and the global nuclear order. Her work has appeared in the Washington Quarterly, War on the Rocks, and the Journal of Strategic Studies. Heather is also a senior associate fellow at the European Leadership Network, an associate fellow at the Royal United Services Institute, and a member of the Wilton Park Advisory Council. She is an adjunct research staff member at the Institute for Defense Analyses (IDA), where she has worked since 2008. Heather has a PhD in war studies from King's College London, an MA in security policy studies from the George Washington University, and a BA in international relations and Russian studies from Boston University.

Suzanne Claeys is a program manager and research associate with the Project on Nuclear Issues at CSIS where she manages the CSIS European Trilateral Track 2 Nuclear Dialogues and research on the future of arms control in an era of strategic competition. Ms. Claeys is an MA and nuclear policy certificate candidate at the Elliott School of International Affairs at the George Washington University. She graduated Phi Beta Kappa from American University with a BA in international studies and Spanish studies.

Endnotes

1 Rebecca Hersman, Eric Brewer, Lindsey Sheppard, and Maxwell Simon, *Influence and Escalation: Implication of Chinese and Russian Influence Operations for Crisis Management* (Washington, DC: CSIS, November 2021), https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/211109_Hersman_Influence_and_Escalation_0.pdf?fAE4qTWKrjF0eT9k8wVV6gs8KDU_x0Bn.

2 "Monitoring Technologies: How They Work," CTBT Organization Preparatory Commission, https://www.ctbto.org/verification-regime/monitoring-technologies-how-they-work/hydroacoustic-monitoring/.

3 Rebecca Hersman, "Wormhole Escalation in the New Nuclear Age," *Texas National Security Review* 3, no. 3 (Summer 2020), https://repositories.lib.utexas.edu/handle/2152/83221.

4 Heather Williams, "Asymmetric arms control and strategic stability: Scenarios for limiting hypersonic glide vehicles," *Journal of Strategic Studies* 42, no. 6 (2019), doi:10.1080/01402390.2019.1627521.

5 "CATALINK," Institute for Science and Technology, accessed November 22, 2021, https://securityandtechnology.org/catalink/.

6 "Keynote Address: Colin Kahl," YouTube video, posted by Carnegie Endowment, June 23, 2021, 36:08, https://www.youtube.com/watch?v=2NSELljDFNk.

7 Office of the Director of National Intelligence, *Annual Threat Assessment of the US Intelligence Community* (Washington, DC: Office of the Directorate of National Intelligence, 2021), 10, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf.

8 Charles Richard, "Testimony on United States Strategic Command and United States Space Command in review of the Defense Authorization Request for Fiscal Year 2022 and the Future Years Defense Program," Testimony before the Senate Armed Services Committee, April 20, 2021, https://www.armed-services.senate.gov/imo/media/doc/21-22_04-20-2021.pdf; and Hans Kristensen and Matt Korda, "Russian nuclear weapons,

2021," *Bulletin of the Atomic Scientists* 77, no. 2 (2021), doi:10.1080/00963402.2021.1885869.

9 For division from Western analysts, see, for example, Olga Oliker and Andret Baklitsky, "The Nuclear Posture Review and Russian 'De-escalation': A Dangerous Solution to a Non-existent Problem," War on the Rocks, February 20, 2018, https://warontherocks.com/2018/02/nuclear-posture-review-russian-de-escalation-dangerous-solution-nonexistent-problem/; and Austin Long, "Russian Nuclear Forces and Prospects for Arms Control," Hearing before the U.S. House of Representatives Committee on Foreign Affairs Subcommittee on Terrorism, Nonproliferation, and Trade, 115th Cong., 2nd sess., June 21, 2018, https://www.congress.gov/115/meeting/house/108459/witnesses/HHRG-115-FA18-Wstate-LongA-20180621.pdf.

10 Olga Oliker, "New Document Consolidates Russia's Nuclear Policy in One Place," Russia Matters, June 4, 2020, https://www.russiamatters.org/analysis/new-document-consolidates-russias-nuclear-policy-one-place.

11 "Relations with Russia," North Atlantic Treaty Organization, n.d., https://www.nato.int/cps/en/natolive/topics_50090.htm.

12 Andrew Kramer, "Fighting Escalates in Eastern Ukraine, Signaling the End to Another Cease-Fire," N*ew York Times*, March 30, 2021, https://www.nytimes.com/2021/03/30/world/europe/ukraine-russia-fighting.html; Tom Balmforth and Matthias Williams, "Russia orders troops back to base after buildup near Ukraine," Reuters, April 22, 2021, https://www.reuters.com/world/europe/russia-orders-troops-back-base-after-buildup-near-ukraine-2021-04-22/; and "Russia shuts mission to NATO in spay row retaliation," Reuters, October 18, 2021, https://www.reuters.com/world/europe/russia-shuts-mission-nato-after-staff-expelled-2021-10-18/.

13 Ibid.

14 U.S. Space Command, "Russia tests direct-ascent anti-satellite missile," Press release, April 15, 2020, https://www.spaceforce.mil/News/Article/2151733/russia-tests-direct-ascent-anti-satellite-missile/.

15 Kaitlyn Johnson, *Key Governance Issues in Space* (Washington, DC: CSIS, September 2020), 19, https://aerospace.csis.org/wp-content/uploads/2020/09/Johnson_GovernanceInSpace_WEB_FINAL-1.pdf.

16 Ibid.

17 Joseph Menn, "Analysis: Murkiness of Russia's ransomware role complicates Biden summit mission," Reuters, June 14, 2021, https://www.reuters.com/technology/murkiness-russias-ransomware-role-complicates-biden-summit-mission-2021-06-14/.

18 Kathleen Hicks et al., *By Other Means Part 1: Campaigning in the Gray Zone* (Washington, DC: CSIS, July 2019), v, https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/Hicks_GrayZone_interior_v4_FULL_WEB_0.pdf.

19 Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China, 2020* (Washington, DC: U.S. Department of Defense, 2020), ix, https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.PDF; Hans M. Kristensen and Matt Korda, "Status of World Nuclear Forces," Federation of American Scientists, n.d., https://fas.org/issues/nuclear-weapons/status-world-nuclear-forces/.

20 Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China, 2021* (Washington, DC: U.S. Department of Defense, 2021), vii, https://media.defense.gov/2021/Nov/03/2002885874/-1/-1/0/2021-CMPR-FINAL.PDF.

21 Joby Warrick, "China is building more than 100 new missile silos in its western desert, analysts say," *Washington Post*, June 30, 2021, https://www.washingtonpost.com/national-security/china-nuclear-missile-silos/2021/06/30/0fa8debc-d9c2-11eb-bb9e-70fda8c37057_story.html; Matt Korda and Hans Kristensen, "China Is Building a Second Nuclear Missile Silo Field," Federation of American Scientists, July 26, 2021,

https://fas.org/blogs/security/2021/07/china-is-building-a-second-nuclear-missile-silo-field/; and Rod Lee, "PLA Likely Begins Construction of an Intercontinental Ballistic Missile Silo Site near Hanggin Banner," Air University's China Aerospace Studies Institute, August 12, 2021, https://www.airuniversity.af.edu/CASI/Display/Article/2729781/pla-likely-begins-construction-of-an-intercontinental-ballistic-missile-silo-si/.

22 Korda and Kristensen, "China Is Building a Second Nuclear Missile Silo Field."

23 Geoff Brumfiel, "A New Tunnel Is Spotted At A Chinese Nuclear Test Site," NPR, July 30, 2021, https://www.npr.org/2021/07/30/1022209337/a-new-tunnel-is-spotted-at-a-chinese-nuclear-test-site.

24 Defense Intelligence Agency, *China Military Power: Modernizing a Force to Fight and Win* (Washington, DC: 2019), ix, https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/China_Military_Power_FINAL_5MB_20190103.pdf; and Richard, "Testimony on United States Strategic Command and United States Space Command."

25 Office of the Director of National Intelligence, *Annual Threat Assessment*, 7.

26 Richard, "Testimony on United States Strategic Command and United States Space Command."

27 Kelley Sayler, *Hypersonic Weapons: Background and Issues for Congress*, CRS Report No. R45811 (Washington, DC: Congressional Research Service, 2021), 15, https://sgp.fas.org/crs/weapons/R45811.pdf.

28 Caitlin Talmadge, *China and Nuclear Weapons* (Washington, DC: Brookings Institute, September 2019), 1, https://www.brookings.edu/wp-content/uploads/2019/09/FP_20190930_china_nuclear_weapons_talmadge-1.pdf.

29 See David Logan, "Dangerous Myths about China's Nuclear Weapons"; and Peter Pry, "China's 'no first use' nuclear fiction."

30 Hicks et al., *By Other Means*, 7.

31 For more on the Belt and Road Initiative, see "How Will the Belt and Road Initiative Advance China's Interests?" *China Power*, CSIS, https://chinapower.csis.org/china-belt-and-road-initiative/.

32 Ibid, 8.

33 Defense Intelligence Agency, *China Military Power*, 46.

34 Todd Harrison et al., *Space Threat Assessment 2020* (Washington, DC: CSIS, March 2020), 18, https://aerospace.csis.org/wp-content/uploads/2020/03/Harrison_SpaceThreatAssessment20_WEB_FINAL-min.pdf; and Ellen Nakashima, "Chinese breach data of 4 million federal workers," *Washington Post*, June 4, 2015, https://www.washingtonpost.com/world/national-security/chinese-hackers-breach-federal-governments-personnel-office/2015/06/04/889c0e52-0af7-11e5-95fd-d580f1c5d44e_story.html.

35 The White House of President Barack Obama, "Fact Sheet: President Xi Jinping's State Visit to the United States," Press release, September 25, 2015, https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.

36 Office of the Director of National Intelligence, *Annual Threat Assessment of the US Intelligence Community* 2021, 8.

37 Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China*, 2021, vii.

38 James Dickinson, "Testimony on United States Strategic Command and United States Space Command in review of the Defense Authorization Request for Fiscal Year 2022 and the Future Years Defense Program," Testimony before the Senate Armed Services Committee, April 20, 2021, https://www.armed-services.senate.

gov/imo/media/doc/21-22_04-20-2021.pdf.

39 Harrison et al., *Space Threat Assessment 2020*, 11.

40 Ibid., 12.

41 Ibid.

42 Stephen Walt, "The Real Reason U.S. Allies Are Upset About Afghanistan," *Foreign Policy*, August 27, 2021, https://foreignpolicy.com/2021/08/27/the-real-reason-u-s-allies-are-upset-about-afghanistan/.

43 David Herszenhorn, "EU Leaders Accuse Biden of Disloyalty to Allies," Politico, September 21, 2021, https://www.politico.eu/article/eu-charles-michel-biden-disloyalty-allies-aukus/.

44 Jim Garamone, "DOD Policy Chief Kahl Discusses Strategic Competition With Baltic Allies," DoD News, September 17, 2021, https://www.defense.gov/News/News-Stories/Article/Article/2780661/dod-policy-chief-kahl-discusses-strategic-competition-with-baltic-allies/.

45 "Secretary of Defense Lloyd J. Austin III Participates in Fullerton Lecture Series in Singapore," U.S. Department of Defense, transcript, July 27, 2021, https://www.defense.gov/News/Transcripts/Transcript/Article/2711025/secretary-of-defense-lloyd-j-austin-iii-participates-in-fullerton-lecture-serie/.

46 "Working Paper: A Nuclear Risk Reduction Package," Stockholm Initiative, 10th Review Conference of the Parties to the Treaty on the Non-Proliferation of Nuclear Weapons, July 2021, https://www.government.se/4a2425/contentassets/690891c6d51244e188aa6e8f2677f57c/workingpapernuclearriskreduction_stockholminitiative_endorsed-by-21-states-july-2021.pdf.

47 Michael Onderco et al., "When do the Dutch want to join the nuclear ban treaty? Findings of a public opinion survey in the Netherlands," *Nonproliferation Review* (October 2021), doi:10.1080/10736700.2021.1978156.

48 Michael Onderco and Michal Smetana, "German views on US nuclear weapons in Europe: public and elite perspectives," *European Security* 30, no. 4, (2021): 630–648, doi:10.1080/09662839.2021.1941896.

49 "Harmel Report," NATO, November 16, 2017, https://www.nato.int/cps/en/natohq/topics_67927.htm.

50 President Joseph R. Biden, *Interim National Security Strategic Guidance* (Washington, DC: The White House, 2021), https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf.

51 "Artificial intelligence (AI) startup funding worldwide from 2011 to 2021 (in billion U.S. dollars), by quarter," Statista, 2021, https://www.statista.com/statistics/943151/ai-funding-worldwide-by-quarter/.

52 Statista Digital Market Outlook, *In-depth Report: Artificial Intelligence 2021* (Hamburg: Statista, August 2021), 35, https://www.statista.com/study/50485/artificial-intelligence/.

53 Jessica Cox and Heather Williams, "The Unavoidable Technology: How Artificial Intelligence Can Strengthen Nuclear Stability," *Washington Quarterly* 44, no. 1 (2021), 79, doi:10.1080/0163660X.2021.1893019?journalCode=rwaq20.

54 Rose Gottemoeller, "The Standstill Conundrum: The Advent of Second-Strike Vulnerability and Options to Address It," *Texas National Security Review* 4, no. 4 (Fall 2021), https://tnsr.org/2021/10/the-standstill-conundrum-the-advent-of-second-strike-vulnerability-and-options-to-address-it/.

55 See for example General Glen VanHerck's, commander of the North American Aerospace Defense Command (NORAD) and the U.S. Northern Command (USNORTHCOM), statements to the House Armed Services Committee in April 2021, https://www.norad.mil/Newsroom/Article/2572565/usnorthcom-and-norad-posture-statement/.

56 See, for example, Michael Horowitz's work on AI.

57 Akira Oikawa and Yuta Shimono, "China overtakes US in AI research," Nikkei Asia, August 10, 2021, https://asia.nikkei.com/Spotlight/Datawatch/China-overtakes-US-in-AI-research.

58 Michael Horowitz, Elsa Kania, Gregory Allen, Paul Scharre, *Strategic Competition in an Era of Artificial Intelligence* (Washington, DC: Center for a New American Security, July 2018), https://www.cnas.org/publications/reports/strategic-competition-in-an-era-of-artificial-intelligence.

59 Sara Hsu, "China and Artificial Intelligence," The Diplomat, April 19, 2021, https://thediplomat.com/2021/04/china-and-artificial-intelligence/.

60 See UNIDIR, *Modernizing Arms Control*; and Jill Hruby and M. Nina Miller, *Assessing and Managing the Benefits and Risks of Artificial Intelligence in Nuclear-Weapon Systems*.

61 For more on emerging technology and dual-use concerns for global public health, see WHO, *Emerging technologies and dual-use concerns: a horizon scan for global public health*.

62 For more on the implications of biotech on strategic stability, see Margaret Kosal, "CRISPR and new genetic-engineering techniques: emerging challenges to strategic stability and nonproliferation."

63 Sriharshita Musunuri et al., "Rapid Proliferation of Pandemic Research: Implications for Dual-Use Risks," *mBio* 12, no. 5 (September/October 2021), doi:10.1128/mBio.01864-21.

64 Rebecca Hersman, Suzanne Claeys, and Cyrus Jabbari, "Chapter 3: Emerging Challenges to the CW System of Restraint," in *Rigid Structures, Evolving Threats: Preventing the Proliferation and Use of Chemical Weapons* (Washington, DC: CSIS, December 2019): 9–27, https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/191218_Hersman_RigidStructures_WEB.pdf?LHDLRedZ2X3eEhGwYz7Ko8lXzSs1hEEO; and Rebecca Hersman and William Pittinos, *Restoring Restraint* (Washington, DC: CSIS, June 2018), https://www.csis.org/analysis/restoring-restraint.

65 Cyrus Jabbari and Philipp C. Bleek, "Honey, I Shrunk the Lab: Emerging Microfluidics Technology and its Implications for Chemical, Biological, and Nuclear Weapons," Center for the Study of Weapons of Mass Destruction, Emergence and Convergence, May 2019, https://wmdcenter.ndu.edu/ Portals/97/EC%20research%20paper%20no%205%20-%20Bleek%20and%20Jabbari.pdf.

66 Mark Bishop, "Chemical Weapons," Institute Bishop, 2019, https://institutebishop.org/chemical_weapons_S&T_short_lecture.pdf.

67 See Ben Buchanan, *The Cybersecurity Dilemma.*

68 Rebecca Hersman, Eric Brewer, Lindsey Sheppard, and Maxwell Simon, *Influence and Escalation: Implication of Chinese and Russian Influence Operations for Crisis Management* (Washington, DC: CSIS, November 2021), https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/211109_Hersman_Influence_and_Escalation_0.pdf?fAE4qTWKrjF0eT9k8wVV6gs8KDU_x0Bn.

69 Ibid.

70 Ibid.

71 Michael Schwirtz, "Top Secret Russian Unit Seeks to Destabilize Europe, Security Officials Say," *New York Times*, October 8, 2019, https://www.nytimes.com/2019/10/08/world/europe/unit-29155-russia-gru.html; Eric Tucker, "US officials: Russia behind spread of virus disinformation," AP News, July 28, 2020, https://apnews.com/article/ap-top-news-health-moscow-ap-fact-check-elections-3acb089e6a333e051dbc4a465cb68ee1; Amy Mackinnon, "What's This Unit of Russian Spies That Keeps Getting Outed?," *Foreign Policy*, July 1, 2020, https://foreignpolicy.com/2020/07/01/what-is-unit-29155-gru-russian-spies-bounties/;

Bellingcat Investigation Team, "Russia's clandestine Chemical Weapons Programme and the GRU's Unit 29155," Bellingcat, October 23, 2020, https://www.bellingcat.com/news/uk-and-europe/2020/10/23/russias-clandestine-chemical-weapons-programme-and-the-grus-unit-21955/; and "Senior GRU Leader Directly Involved With Czech Arms Depot Explosion," Bellingcat, April 20, 2021, https://www.bellingcat.com/news/2021/04/20/senior-gru-leader-directly-involved-with-czech-arms-depot-explosion/.

72 Government of the Netherlands, "Netherlands Defence Intelligence and Security Service disrupts Russian cyber operation targeting OPCW," Press release, October 4, 2018, https://www.government.nl/latest/news/2018/10/04/netherlands-defence-intelligence-and-security-service-disrupts-russian-cyber-operation-targeting-opcw.

73 Leanne Quinn, "45 OPCW States Demand Answers About Navalny," Arms Control Today, November 2021, https://www.armscontrol.org/act/2021-11/news/45-opcw-states-demand-answers-about-navalny.

74 Ibid.

75 Search was conducted on November 5, 2021, using "OPCW" in the Google News search bar. Results may vary based on many factors, such as time of search, IP address or VPN use, language, cookies, and browsing history, among others.

76 Office of the Secretary of Defense, *Military and Security Developments Involving the People's Republic of China* 2021, 64.

77 See Jessica Brandt and Torret Taussig, "The Kremlin's disinformation playbook goes to Beijing," Brookings, May 19, 2020, https://www.brookings.edu/blog/order-from-chaos/2020/05/19/the-kremlins-disinformation-playbook-goes-to-beijing/.

78 See https://datayo.org/ for more OSINT examples.

79 Hersman et al., *Rigid Structures, Evolving Threat*.

80 Reid Pauly, Twitter post, October 27, 2021, 12:04 p.m., https://twitter.com/reidpauly/status/1453392186700095494.

81 Ned Beauman, "How to Conduct Open-Source Investigation, According to the Founder of Bellingcat," *New Yorker*, August 30, 2018, https://www.newyorker.com/culture/culture-desk/how-to-conduct-an-opensource-investigation-according-to-the-founder-of-bellingcat.

82 "Open Nuclear Network's Code of Ethics," Open Nuclear Network, June 25, 2020, https://oneearthfuture.org/program/open-nuclear-network/code-of-ethics.

83 "Monitoring Technologies: How They Work," CTBT Organization Preparatory Commission, https://www.ctbto.org/verification-regime/monitoring-technologies-how-they-work/hydroacoustic-monitoring/.

84 Michael P. Gleason and Luc H. Riesbeck, *Noninterference with National Technical Means: The Status Quo Will Not Survive* (El Segundo, CA: Aerospace Corporation, January 2020), 2, https://aerospace.org/sites/default/files/2020-01/Gleason_NTM_20200114.pdf.

85 National Academies of Sciences, Engineering, and Medicine, *Nuclear Proliferation and Arms Control Monitoring, Detection, and Verification: A National Security Priority: Interim Report* (Washington, DC: The National Academies Press, April 2021), https://www.nap.edu/read/26088/chapter/1.

86 "Overview of the Verification Regime," Comprehensive Test Ban Treaty, n.d., https://www.ctbto.org/verification-regime/background/overview-of-the-verification-regime/.

87 James Acton, "Escalation through Entanglement: How the Vulnerability of Command-and-Control Systems

Raises the Risks of an Inadvertent Nuclear War," *International Security* 43, no. 1 (2018), doi:10.1162/isec_a_00320.

88 Ian Bowers, "Escalation at Sea," *Naval War College Review* 71, no. 4 (Autumn 2018): 61, https://www.jstor.org/stable/26607089.

89 Hersman, "Wormhole Escalation in the New Nuclear Age."

90 Heather Williams, "Russia Still Needs Arms Control," *Arms Control Today* 46, no. 1 (January/February 2016), https://www.armscontrol.org/act/2016-01/features/russia-still-needs-arms-control.

91 Eugene Rumer, *Russia, and the Security of Europe* (Washington, DC: Carnegie Endowment for International Peace, June 2016), 4, https://carnegieendowment.org/files/CP_276_Rumer_Russia_Final.pdf.

92 U.S. Department of State, *2021 Adherence to and Compliance With Arms Control, Nonproliferation, and Disarmament Agreements and Commitments* (Washington, DC: U.S. Department of State, 2021), https://www.state.gov/2021-adherence-to-and-compliance-with-arms-control-nonproliferation-and-disarmament-agreements-and-commitments/.

93 Mark B. Schneider, "Russia Cheats," *Air Force Magazine*, July 2016, https://www.nipp.org/wp-content/uploads/2016/07/Schneider-Russia-Cheats.pdf.

94 China is signatory to the Non-Proliferation Treaty (NPT), the Comprehensive Test Ban Treaty (CTBT), participant in all four Nuclear Security Summits, played a key role in hosting and mediating the Six-Party Talks to denuclearize North Korea, and took part in the negotiations on the Joint Comprehensive Plan of Action (JCPOA) to limit Iran's nuclear capabilities. "Arms Control and Proliferation Profile: China," Arms Control Association, last reviewed July 2017, https://www.armscontrol.org/factsheets/chinaprofile.

95 Henrik Stålhane Hiim and Magnus Langset Trøan, "China's Atomic Pessimism and the Future of Arms Control," War on the Rocks, June 21, 2021, https://warontherocks.com/2021/06/chinas-atomic-pessimism-and-the-future-of-arms-control/.

96 Tong Zhao, "Opportunities for Nuclear Arms Control Engagement with China," Arms Control Association, January/February 2020, https://www.armscontrol.org/act/2020-01/features/opportunities-nuclear-arms-control-engagement-china; and ibid.

97 Fu Cong, "The Future of Arms Control and Non-Proliferation Regime," (speech, 2019 Moscow Non-Proliferation Conference, Moscow, November 8, 2019), https://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1714403.shtml.

98 See Tong Zhao, "Practical Ways to Promote U.S.-China Arms Control Cooperation"; and Fiona Cunningham, "Cooperation under Asymmetry? The Future of US-China Nuclear Relations," *Washington Quarterly* 44, no. 2 (June 12021), doi:10.1080/0163660X.2021.1934253.

99 Fu Cong, "Dialogue between the P5 Delegations and Academia," (speech, February 2, 2019), https://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1635178.shtml.

100 Sarah Kreps, "The Institutional Design of Arms Control Agreements," *Foreign Policy Analysis* 14, no. 4 (January 2018): 144, doi:10.1093/fpa/orw045.

101 Vince Manzo, *Nuclear Arms Control Without a Treaty? Risks and Options After New START* (Washington, DC: CNA, March 2019), 2, https://www.cna.org/CNA_files/PDF/IRM-2019-U-019494.pdf.

102 Theresa Hitchens, "UN Committee Votes 'Yes' On UK-US-Backed Space Rules Group," Breaking Defense, November 1, 2021, https://breakingdefense.com/2021/11/un-committee-votes-yes-on-uk-us-backed-space-rules-group/.

103 Gabriele Kraatz-Wadsack, "Monitoring and Verification in the Biological-Weapons Area," *The Nonproliferation Review* (February 2021), doi:10.1080/10736700.2020.1865629.

104 *Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and on Their Destruction*, Art. 5, March 1, 1999, https://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg_no=XXVI-5&chapter=26&clang=_en.

105 Cox and Williams, "The Unavoidable Technology."

106 Ibid.

107 "About IPNDV," IPNDV, n.d., https://www.ipndv.org/about/.

108 *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies*, Art. IX, December 19, 1996, https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/outerspacetreaty.html.

109 Heather Williams, "Asymmetric arms control and strategic stability: Scenarios for limiting hypersonic glide vehicles," *Journal of Strategic Studies* 42, no. 6 (2019), doi:10.1080/01402390.2019.1627521.

110 "CATALINK," Institute for Science and Technology, accessed November 22, 2021, https://securityandtechnology.org/catalink/.

111 "The Scale and Logic of Chemical Weapons Use in Syria," Global Public Policy Institute, n.d., https://www.gppi.net/2020/04/20/the-scale-and-logic-of-chemical-weapons-use-in-syria.

112 Russian Embassy, Twitter post, April 17, 2018, 7:56 a.m., https://twitter.com/RussianEmbassy/status/986211672770609153; and "Syrian Army Discovers White Helmets' Filming Site in Eastern Ghouta," Sputnik News, April 10, 2018, https://sputniknews.com/middleeast/201804101063422215-white-helmets-fake-video-site/.

113 Lukas Andriukaitis et al., *Breaking Ghouta* (Washington, DC: Atlantic Council, September 2018), 71, https://www.atlanticcouncil.org/wp-content/uploads/2019/08/Breaking-Ghouta_English.pdf.

114 Jack O. Nassetta and Ethan P. Fecht, *All the World is Staged: An Analysis of Social Media Influence Operations against US Counterproliferation Efforts in Syria* (Monterey, CA: James Martin Center for Nonproliferation Studies, 2018), https://www.nonproliferation.org/wp-content/uploads/2018/09/op37-all-the-world-is-staged.pdf.

115 "How the Dutch foiled Russian 'cyber-attack' on OPCW," BBC News, October 4, 2018, https://www.bbc.com/news/world-europe-45747472.

116 Dr. Kate Starbird, among others, has written about the intersections between organic online activism, government-controlled media, computational propaganda, and other state-directed efforts to infiltrate, shape, and weaponize sources with independent political beliefs. See Kate Starbird et al., "Ecosystem or Echo-System? Exploring Content Sharing across Alternative Media Domains," *Proceedings of the International AAAI Conference on Web and Social Media*, 12, no. 1 (2018), http://faculty.washington.edu/kstarbi/Starbird-et-al-ICWSM-2018-Echosystem-final.pdf.

117 Organisation for the Prohibition of Chemical Weapons, "Independent Investigation into Possible Breaches of Confidentiality Report Released," Press release, February 6, 2020, https://www.opcw.org/media-centre/news/2020/02/opcw-independent-investigation-possible-breaches-confidentiality-report.

118 Susan Sarandon, Twitter post, May 8, 2020, 3:10 p.m., https://twitter.com/SusanSarandon/status/1258836672856428546.

119 "Note by the Technical Secretariat: Work of the Investigation and Identification Team Established by Decision C-SS-4/DEC.3 (Dated 27 June 2018)," OPCW Executive Council, June 28, 2019, https://www.opcw.org/sites/default/files/documents/2019/07/ec91s03%28e%29.pdf.

120 Technical Secretariat of OPCW, *First Report by the OPCW Investigation And Identification Team "Addressing The Threat From Chemical Weapons Use" Ltamenah (Syrian Arab Republic) 24, 25, And 30 March 2017* (The Hague: April 8, 2020), https://www.opcw.org/sites/default/files/documents/2020/04/s-1867-2020%28e%29.pdf; and Technical Secretariat of OPCW, *Second Report by the OPCW Investigation And Identification Team "Addressing The Threat From Chemical Weapons Use" Saraqib (Syrian Arab Republic) – 4 February 2018* (The Hauge: April 12, 2021), https://www.opcw.org/sites/default/files/documents/2021/04/s-1943-2021%28e%29.pdf.

121 "Conference of the States Parties adopts Decision to suspend certain rights and privileges of the Syrian Arab Republic under the CWC," OPCW, April 22, 2021, https://www.opcw.org/media-centre/news/2021/04/conference-states-parties-adopts-decision-suspend-certain-rights-and.

122 Ibid.

123 "Syria stripped of rights at chemical weapons watchdog," AFP, April 21, 2021, https://www.france24.com/en/live-news/20210421-syria-stripped-of-rights-at-chemical-weapons-watchdog.

124 Quinn, "45 OPCW States Demand Answers About Navalny."

125 Ibid.

126 Bellingcat Investigation Team, "Open Source Survey of Alleged Chemical Attacks in Douma on 7th April 2018," Bellingcat, April 11, 2018, https://www.bellingcat.com/news/mena/2018/04/11/open-source-survey-alleged-chemical-attacks-douma-7th-april-2018/.

127 Technical Secretariat of OPCW, *Interim Report Of The OPCW Fact-finding Mission In Syria Regarding The Incident Of Alleged Use Of Toxic Chemicals As A Weapon In Douma, Syrian Arab Republic, On 7 April 2018* (The Hague: July 6, 2018), https://www.opcw.org/sites/default/files/documents/S_series/2018/en/s-1645-2018_e_.pdf; and Technical Secretariat of OPCW, Rep*ort Of The Fact-finding Mission Regarding The Incident Of Alleged Use Of Toxic Chemicals As A Weapon In Douma, Syrian Arab Republic, On 7 April 2018* (The Hague: March 1, 2019), https://www.opcw.org/sites/default/files/documents/2019/03/s-1731-2019%28e%29.pdf.

128 Bellingcat Investigation Team, "The OPCW Douma Leaks Part 1: We Need to Talk About 'Alex'," Bellingcat, January 15, 2020, https://www.bellingcat.com/news/mena/2020/01/15/the-opcw-douma-leaks-part-1-we-need-to-talk-about-alex/; and Bellingcat Investigation Team, "The OPCW Douma Leaks Part 2: We Need To Talk About Henderson," Bellingcat, January 17, 2020, https://www.bellingcat.com/news/mena/2020/01/17/the-opcw-douma-leaks-part-2-we-need-to-talk-about-henderson/.

129 "Bellingcat," Bellingcat, https://www.bellingcat.com/about/.

130 Sarah Jacobs Gamberini and Amanda Moodie, "Bioweapons Accusations in Today's Covid-19 Conspiracy Theories," War on the Rocks, April 6, 2020, https://warontherocks.com/2020/04/the-virus-of-disinformation-echoes-of-past-bioweapons-accusations-in-todays-covid-19-conspiracy-theories/.

131 Anna Schecter, "China launches new Twitter accounts, 90,000 tweets in COVID-19 info war," NBC News, May 20, 2020, https://www.nbcnews.com/news/world/china-launches-new-twitter-accounts-90-000-tweets-covid-19-n1207991.

132 Erika Kinetz, "Anatomy of a conspiracy: With COVID, China took leading role," AP, February 15, 2021, https://apnews.com/article/pandemics-beijing-only-on-ap-epidemics-media-122b73e134b780919cc1808f3f6f16e8.

133 Belén Carrasco Rodríguez, *Information Laundering in Germany* (Riga, Latvia: NATO STRATCOM COE, October 2020), https://stratcomcoe.org/publications/information-laundering-in-germany/23.

134 Jane Lytvynenko, "The 'Plandemic' Video Has Exploded Online—And It Is Filled With Falsehoods," BuzzFeed News, May 7, 2020, https://www.buzzfeednews.com/article/janelytvynenko/coronavirus-plandemic-viral-harmful-fauci-mikovits.

135 Ibid.; and Sheera Frenkel, Ben Decker, and Davey Alba, "How the 'Plandemic' Movie and Its Falsehoods Spread Widely Online," *New York Times*, May 21, 2020, https://www.nytimes.com/2020/05/20/technology/plandemic-movie-youtube-facebook-coronavirus.html.

136 "COVID-19 shows why united action is needed for more robust international health architecture," World Health Organization, March 30, 2021, https://www.who.int/news-room/commentaries/detail/op-ed---covid-19-shows-why-united-action-is-needed-for-more-robust-international-health-architecture.

COVER PHOTO PETER JURIK/ADOBE STOCK

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

1616 Rhode Island Avenue NW
Washington, DC 20036
202 887 0200 | **www.csis.org**

ROWMAN & LITTLEFIELD

Lanham • Boulder • New York • London

4501 Forbes Boulevard
Lanham, MD 20706
301 459 3366 | **www.rowman.com**

ISBN 978-1-5381-4052-9