MULTI-DOMAIN COMPLEXITY AND STRATEGIC STABILITY IN PEACETIME, CRISIS, AND WAR

Annotated Bibliography

February 2021

Center for Global Security Research
LAWRENCE LIVERMORE NATIONAL LABORATORY

Annotated Bibliography

Multi-domain Complexity and Strategic Stability in Peacetime, Crisis, and War

Center for Global Security Research
Livermore, California, February 2021

Prepared By:
Jacek Durkalec with Zachary Davis, Lauren Borja, Krystyna Marcinek,
Anna Peczeli, Brian Radzinsky, and Brandon Williams

Introduction by Brad Roberts

The expansion of military competition into new technical domains, such as cyber space and outer space, has generated a sharp rise of concern about the implications of such competition and capabilities for strategic stability. This concern is reflected in a parallel explosion of scholarship aimed at understanding the nature of these new forms of competition, the associated risks, and possible means to reduce or eliminate those risks. The resulting studies and publications have grown rapidly in number, generating many valuable insights and policy recommendations. But the volume of literature has grown to the point where it is overwhelming for the interested non-specialist seeking to undertand the main insights and main currents of debate. Moreover, for the interested policymaker, the literature tends to fall short in two ways. Much of the academic literature is highly specialized, making it somewhat inaccessible for the non-specialist. And it focuses heaviliy on individual technologies rather than on their complex interactions, as the policymaker experiences them.

In an effort to illuminate those main insights and currents of debate, we have selected a portion of the literature (approximately 75 items) and organized it in a taxonomic structure. Our selection of literature has emphasized items that look beyond individual technologies and their impacts to explore complex interactions among multiple technologies. We have also emphasized items that develop core propositions about impacts on strategic stability. We have not sought to identify every study advancing a particular line of argument, on the argument that one or two were sufficient for the intellectual map we have tried to assemble. We have drawn on English-language sources, including many from Europe. We recognize that there is a significant literature being generated by Russian, Chinese, and other non-Western experts, including by U.S. allies in East Asia, and envision exploring that literature as a possible follow-on activity. This document draws on literature available as of the end of 2020.

The taxonomy developed here draws on the spectrum of conflict. That spectrum consists of three phases: peacetime, crisis, and war. Following the primary interest of analysts in war-time

implications, we take these phases in reverse order: war, crisis, and peacetime. In each phase, we have identified in the literature a small number of potential impacts of "emerging and disruptive technologies" on the requirements of strategic stability. The structure of the bibliography follows below.

This bibliography has been developed in partnership with the European Leadership Network and Dr. Andrew Futter of the University of Leicester as an input to a joint effort to create a baseline of shared understanding about multi-domain complexity, strategic stability, and risk mitigation strategies. The views expressed here are solely those of the authors and should not be attributed to the laboratory, any of its sponsors, or its partners in this project.

Structure

Multi-domain Warfare and Escalation, De-Escalation, and War Termination

1. Impacts on the initiation of war
2. Impacts on the perceived value and necessity of preemption
3. Impacts on the control of war
    a. On the time to deliberate
    b. On escalation dynamics
    c. On wartime diplomacy
    d. On the ability to integrate for strategic effects
4. Impacts on the incentives for nuclear employment
5. Impacts on the restoration of deterrence
    a. On assured nuclear retaliation
    b. On continuity of government
6. Impacts on de-escalation and war termination

Multi-domain Deterrence and Crisis Management

1. Impacts of new technologies on the ability to assess the adversary's course of action
2. Impacts on the ability to consult and deliberate
3. Impacts on signaling to adversaries and allies
4. Impacts on the ability to integrate operations for strategic effect

Multi-domain Competition and Peacetime Rivalry

1. Impacts on the ability to gain new advantages of political or military consequence
2. Impacts on the willingness to commit to mutual restraint
3. Impacts on the ability to verify treaty compliance
4. Impacts on alliances and coalitions

Multi-domain Warfare and Escalation, De-Escalation, and War Termination

1. Impacts on the initiation of war

Core propositions in the literature:

- Multidomain warfare will increase incentives for early, decisive action
- Multidomain warfare will compress decision time while adding to the fog of war
- Multidomain warfare will have effects more evolutionary than revolutionary on the initiation of war

Gartzke, Erik and Jon R. Lindsay. "The Cyber Commitment Problem and the Destabilization of Nuclear Deterrence." In *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations*, edited by Lin, Herbert and Amy Zegart. Washington, D.C.: Brookings Institution Press (2018). 195-234.

> Gartzke and Lindsay argue that the secrecy required to develop offensive cyber capabilities can weaken nuclear deterrence and generate first strike incentives. First, the introduction of offensive cyber capabilities to the nuclear domain creates a unique challenge the authors refer to as the "cyber commitment problem." In essence, the secrecy required for successful cyber attacks limits the ability of cyber powers to make deterrent threats that could reveal the existence of an offensive capability. Second, the clandestine nature of cyber operations means that the target of cyber attacks may not detect cyber compromise of their nuclear forces, and may result in more aggressive behavior than its military capabilities would allow.

Horowitz, Michael C. "When speed kills: Lethal autonomous weapon systems, deterrence and stability." *Journal of Strategic Studies* 42, no. 6 (2019): 764-788. DOI: 10.1080/01402390.2019.1621174.

> Horowitz posits that adding autonomy to unmanned kinetic systems gives "speed-based edge in decion-making and reaction times" and the persistence in performing tasks without human cognitive limitations; it also reduces the size of military workforce. However, there are also significant risks of unintended behaviors and accidents due to their complexity. Horowitz asserts that contrary to many popular beliefs, the impact of autonomous weapon systems of interstate wars will be modest, because they don't change fundamental political reasons countries may have to go to war and the uncertainty about their performance will likely lead to caution in the deployment.

Horowitz, Michael C., Paul Scharre, and Ben FitzGerald. "Drone Proliferation and the Use of Force: An Experimental Approach." Washington, DC: Center for a New American Security, 2017. http://drones.cnas.org/wp-content/uploads/2017/03/Drone-Proliferation-and-the-Use-of-Force-Proliferated-Drones.pdf.

> The authors used a survey experiment to examine whether widespread availability of drones could incentivize adventurism and conflict. The study found that using drones instead of manned aircraft increased respondents' willingness to deploy an aircraft into a contested area and shoot down another country's aircraft. However, access to drones

also decreased respondents' willingness to escalate in response to one's aircraft being shot down. Some of these results varied by particular individuals sampled. A sample of Indian respondents found a greater willingness to manned capabilities , which suggests that different cultures or other contextual factors could affect the psychological relationship between drones and a willingness to use force.

Leys, Nathan. "Autonomous Weapon Systems and International Crises." *Strategic Studies Quarterly* (Spring 2018). https://www.airuniversity.af.mil/Portals/10/SSQ/documents/Volume-12_Issue-1/Leys.pdf?ver=2018-02-14-165959-950.

Leys examines the major approaches and debates regarding autonomous weapons systems, exploring 1) competiting defintions of autonomy; 2) the technological challenges surrounding the identification of targets, the potential for miscalculation, and the proliferation of autonomous weapons systems, and 3) the challenges of command and control and integration into the broader military. The author then considers the implications of autonomous weapons for strategic interaction in conflict and highlights potential escalation pathways.

Lowther, Adam and Curtis McGriffin. "America Needs a 'Dead Hand'." *War on the Rocks*. August 16, 2019. https://warontherocks.com/2019/08/america-needs-a-dead-hand/.

The authors observe that as conventional warfare becomes more dependent on high-speed, stealthy or hard-to-track strike systems, decision makers are likely to have less time to make deliberate decisions, such whether to authorize a retaliatory nuclear attack. This situation, the authors argue, can imperil the survivability of nuclear forces because adversaries may be able to neutralize U.S. deterrent forces before the President could issue a nuclear use authorization. The authors argue that an AI-based automated system could provide a stabilizing solution. The authors do not analyze the potential design for such a system, arguing instead that, given the limited alternatives, an automated retaliatory option should be considered as a possible solution to compressed decision times.

2. On the perceived value and necessity of preemption

Core propositions in the literature:

- Multidomain warfare will increase the perceived value of preemption by increasing the first-mover advantage and improving the prospects for success with improved targeting
- Multidomain warfare will reduce the perceived value of preemption by decreasing the prospects for success with improved survivability
- Multidomain warfare will reduce the perceived value of preemption because no actor can escape mutual vulnerability

Center for Global Security Research, Lawrence Livermore National Laboratory. *5th Annual LLNL Deterrence Workshop Multi-Domain Strategic Competition: Rewards and Risks.* Workshop Summary. Livermore, California: CGSR, November 2018. https://cgsr.llnl.gov/content/assets/docs/Deterrence_Workshop_Summary_Final2018.pdf.

> In a 2018 CGSR workshop, participants postulated that multi-domain strategic competition is likely to undermine crisis stability. First, the deepening operational and strategic entanglement of nuclear and non-nuclear weaponry may create stronger incentives for nuclear use. Persistent vulnerability of space-based systems and computer networks can in turn weaken the survivability of nuclear deterrent forces. There are also other potential sources of instability, including exaggerated confidence in the ability to control escalation in grey-zone competitions, and the temptation of third parties to use cyber or other tools to escalate a crisis between two powers. At the same time, participants identified potential countervailing trends, including growing appreciation of shared vulnerability in cyber and outer space.

Garfinkel, Ben, and Allan Dafoe. "How does the offense-defense balance scale?." *Journal of Strategic Studies* 42, no. 6 (2019): 736-763. https://doi.org/10.1080/01402390.2019.1631810.

> The offense-defense balance is a term used to capture the relative ease of attacking vs. defending given available military technology. The authors investigate whether the same proposition holds true as investments and force sizes increase. The authors find that while greater investments can initially improve offensive capability, eventually further investment can shift the balance toward the defensive. For some technologies, such as drone swarms or AI-enabled cyber vulnerability detectors, it may be possible to scale up investments to the point that the defense could dominate.

Gartzke, Erik, and Jon R. Lindsay. “Thermonuclear Cyberwar.” *Journal of Cybersecurity* 3, no.1 (2017): 37-48. https://doi.org/10.1093/cybsec/tyw017.

> Garztke and Lindsay argue that the introduction of cyber warfare into the strategic level of warfare creates new pathways to crisis instability. Because cyber advantages must be kept secret, states are likely to be uncertain about their ability to use cyber capabilities to attack adversary nuclear forces and defend their own deterrents. This increased uncertainty about the nuclear/cyber balance of power raises the risk of miscalculation during a brinksmanship crisis. As a result, the authors argue, we should expect strategic stability in nuclear dyads to be, in part, a function of relative offensive and defensive cyber capacity.

Miller, Jr., James N., and Richard Fontaine. *A New Era in U.S.-Russian Strategic Stability: How Changing Geopolitics and Emerging Technologies are Reshaping Pathways to Crisis and Conflict.* Washington, DC: Center for a New American Security, September 2017. https://s3.amazonaws.com/files.cnas.org/documents/CNASReport-ProjectPathways-Finalb.pdf?mtime=20170918101504.

Miller and Fontaine argue that parallel political, military and technological trends in the U.S.-Russian relationship are leading to the potential for significant crisis instability and first-strike incentives. First, deepening mistrust since the 2010s is fueling investments in military technologies while reducing the scope for diplomatic resolutions to disputes. Second, both sides are likely to have strong incentives to engage in significant attacks in cyber space and outer space in the early phases of a conflict. While each side may rationally conclude that such non-kinetic attacks are less escalatory than the alternatives, the results of such attacks might incentivize inadvertent escalation. Finally, each side's development of modernized strategic offensive and defensive weapons may weaken each side's confidence in their strategic deterrents.

Schneider, Jacquelyn. "The Capability/Vulnerability Paradox and Military Revolutions: Implications for Computing, Cyber, and the Onset of War." *Journal of Strategic Studies* 42, no. 6 (2019): 841–863. DOI: 10.1080/01402390.2019.1627209.

Revolutions in military technology can dramatically change the conduct of war and therefore the balance of power between states. However, the author argues that some military revolutions can make states dependent on critical resources, such as oil. This dependence creates exploitable vulnerabilities that can create incentives for preemptive action. First strike incentives are strongest, Schneider argues, when a revolutionary technology creates high dependence on a particular resources *and* when adversaries have a high ability to affect the use of this resource. The author considers the implications of this framework for network-centric warfare and cyber warfare, arguing that first strike incentives might increase as modern militaries become both more dependent on information and more capable of offensive cyber operations.

3. Impacts on the control of war

Core propositions in the literature:

- Multidomain warfare will reduce control of war by reducing the time to deliberate and complicating the task of reading an adversary's intent
- Multidomain will improve the ability to control war for those with the superior ability to integrate operations and effects
- Multidomain warfare will increase the risks of unwanted escalation by contributing to a false sense of confidence in the ability to control escalation with more information and more options

a. On the time to deliberate

Chambers, William A, John K. Warden, Caroline A. Milne and James A. Blackwell. *Presidential Decision Time Regarding Nuclear Weapons Employment: An Assessment and Options.* Alexandria, VA: Institute for Defense Analyses, 2019.

The authors undertook a study to analyze the time-pressures associated with nuclear use decision making and suggest ways to reduce risks and the time pressures associated with nuclear use decisions. The authors found that while the United States does not anticipate

the prompt use of nuclear weapons (that is, a launch that follows shortly after a decision), credibly signaling that the United States retains such a capability could complicate adversary planning. Prompt launch also provides the president with flexible options if deterrence fails. The authors then discuss ways to increase decision time and reduce miscalculation and other risks.

Speier, Richard H., George Nacouzi, Carrie Lee, and Richard M. Moore. "Hypersonic Missile Nonproliferation: Hindering the Spread of a New Class of Weapons." Santa Monica, CA: RAND Corporation, 2017. https://www.rand.org/pubs/research_reports/RR2137.html.

The spread of high-speed missile systems could pose a threat to U.S. conventional and nuclear forces while exacerbating strategic instability with respect to other nuclear powers. The authors present a two-tiered strategy for limiting hypersonic weapons proliferation. First, they recommend denying exports of complete hypersonic delivery vehicles and enough major subsystems to effectively provide access to complete hypersonic missiles. Second, given dual-use concerns, they recommend a policy of case-by-case export reviews for scramjets and other hypersonic engines and components as well as enabling technologies and resources. As a first step they encourage the U.S., Russia and China to agree not to export complete hypersonic missiles or their major subsystems.

b. On escalation dynamics

Morgan, Forrest E., Karl P. Mueller, Evan S. Medeiros, Kevin L. Pollpeter, and Roger Cliff. "Chapter 6: Managing Escalation in a Complex World" in *Dangerous Thresholds: Managing Escalation in the 21st Century*. Santa Monica, California: RAND Corporation, 2008. https://www.rand.org/content/dam/rand/pubs/monographs/2008/RAND_MG614.pdf.

This far-reaching study takes a deep dive into the concept and literature on escalation with an aim to identifying strategies for escalation management and escalation dominance for U.S. policy makers. The authors first investigate the nature of escalation and its relationship to deterrence, coercion and related concepts. They then consider contemporary escalation risks and offer options for managing escalations and securing U.S. interests.

Talmadge, Caitlin. "Emerging technology and intra-war escalation risks: Evidence from the Cold War, implications for today." *Journal of Strategic Studies* 42, no. 6 (2019): 864- 887. https://doi.org/10.1080/01402390.2019.1631811.

The author develops a framework to examine the impact of emerging technologies on intra-war escalation. Talmadge proposes two causal chains, with the technology as an independent variable (inadvertent escalation) or intervening variable (intentional escalation), respectively. The author applies the framework to three Cold War era case studies: intentional US nuclear escalation in 1950-60s in Europe, inadvertent Soviet and US nuclear escalation in 1980s Europe, and intentional US conventional escalation duing the Vietnam War. Talmadge concludes that emerging technologies are more likely to

serve as an enabler of preexisting intra-war escalation pressures that to be their source and root cause.

c. On wartime diplomacy

Nautilus Institute, Stanley Center for Peace and Security, and Technology for Global Security. "Last Chance: Communicating at the Nuclear Brink Scenarios and Solutions Workshop Synthesis Report." May 14, 2020. https://securityandtechnology.org/wp-content/uploads/2020/07/synthesis_report_last_chance_final_report_IST.pdf.

This report presents a novel solution to the problem of crisis or wartime diplomacy in a degraded communications environment, such as the kind that would accompany the widespread use of cyber or counter-space attacks. The solution would be to develop a highly reliable communications system termed CATALINK to link nuclear National Command Authorities. The report outlines a series of measures that would ensure the reliability, availability and integrity of the CATALINK system and provides a high-level overview of the system's potential architecture.

d. On the ability to integrate for strategic effects

Bracken, Paul. *The Hunt for Mobile Missiles: Nuclear Weapons, AI and the New Arms Race.* Philadelphia, PA: Foreign Policy Research Institute, 2020. https://www.fpri.org/wp-content/uploads/2020/09/the-hunt-for-mobile-missiles.pdf.

Bracken examines trends in the ability of some states to track mobile missiles, which are integral the survivability of Chinese, North Korean and Russian nuclear forces. The ability to successfully hunt for mobile missiles has significant implications for a state's ability to gain nuclear superiority. The hunt for mobile missiles also serves as a case study or "exemplar" of the impact of new technologies on stability and the conduct of war. Bracken argues that the integration of multiple technologies and information streams is dramatically improving the ability to detect and track mobile missiles in near-real time. The report also encourages analysts to adopt frameworks from business to better understand the impact of emerging technologies. He specifically focuses on three concepts useful to understanding technological integration: touchpoints, information chains and value chains. Bracken argues that technological competition is now best thought of as a contest between value chains, rather than between technologies per se.

Roberts, Brad. *Toward New Thinking About Our Changed and Changing World: A Five-Year CGSR Progress Report.* Livermore, California: CGSR, October 2020. https://cgsr.llnl.gov/content/assets/docs/CGSRfiveDIGITAL.pdf.

This paper summarizes key insights gained by CGSR research conducted between 2015 and 2020, including its work on integrated strategic deterrence. One the one hand, CGSR findings indicate that competition and conflict in new domains bring new risks as bold action in cyber and/or outer space very early in a conflict intended to achieve decisive effects may instead incite unwanted escalation. On the other hand, integration offers

many potential benefits, adding to the non-nuclear means of deterrence, defense and, if necessary, escalation. Still, the barriers to integration are numerous, including secrecy, stovepipes, and limited bandwidth.

Warden, John K. "Conventional-Nuclear Integration in the Next National Defense Strategy." Washington, DC: Center for a New American Security, 2020, https://www.cnas.org/publications/commentary/conventional-nuclear-integration-in-the-next-national-defense-strategy.

The author argues that the next U.S. National Defense Strategy (NDS) should prioritize conventional-nuclear integration to deter limited adversary aggression that is backed by threats of escalation, including across the nuclear threshold. Warden posits that refined strategy, improved deliberate and adaptive combatant command plans, adapted doctrine and operational concepts, as well as appropriate mix of capabilities could enable the United States and its allies to achieve U.S. objectives in multidomain conflict while minimizing the risk of nuclear escalation.

4. Impacts on the incentives for nuclear employment

Core propositions in the literature:

- Multi-domain warfare will increase the risk of nuclear use by entangling conventional and nuclear operations
- Multi-domain warfare will reduce the risk of nuclear use by increasing the number and availability of non-nuclear response options

Acton, James M. "Escalation through Entanglement: How the Vulnerability of Command-and-Control Systems Raises the Risks of an Inadvertent Nuclear War." *International Security* 43, no. 1 (August 2018): 56–99. https://www.mitpressjournals.org/doi/pdf/10.1162/isec_a_00320.

Acton examines the pathways through which non-nuclear attacks could lead to nuclear use, particularly in the context of a conventional war. Three pathways to inadvertent nuclear use are identified: 1) through *misinterpreted warning*—a misinterpretation of the intent behind an adversary's imminent attack; 2) through a concern that an adversary's actions will preclude the escalating actor's efforts to limit damage from a nuclear attack; and 3) by creating incentives for either side to use its nuclear weapons first lest its adversary's efforts deny it the ability to retaliate later. Acton recommends reducing the risk of inadvertent escalation by segmenting nuclear weapons and command and control systems from non-nuclear military forces.

See also: *Entanglement: Chinese and Russian Perspectives on Non-nuclear Weapons and Nuclear Risks.* Edited by James M. Acton. Washington DC: Carnegie Endowment for International Peace, November 2017. https://carnegieendowment.org/files/Entanglement_interior_FNL.pdf.

Cunningham, Fiona S.; Taylor M. Fravel. "Dangerous Confidence? Chinese Views on Nuclear Escalation." *International Security* 44, no. 2 (Fall 2019): 61-109. https://www.mitpressjournals.org/doi/full/10.1162/isec_a_00359.

> Cunningham and Fravel interviewed Chinese experts to assess their views on escalation control in conventional conflicts. In general, they found that Chinese experts and strategic writing expresses high confidence in China's ability to control the pace and scope of a conventional war. Chinese thinkers, in contrast, are skeptical of their ability to control nuclear escalation, a belief that may further encourage the belief that conventional wars can be kept limited and below the nuclear threshold. This confidence in conventional escalation control could create unanticipated pathways for nuclear escalation. In addition, the prominence of technologies such as counter-space weapons and offensive cyber weapons in Chinese strategy could create additional pathways to escalation in a U.S.-China conflict—pathways that may not be prominent in the minds of Chinese thinkers.
>
> See also: Zhao, Tong. "Conventional long-range strike weapons of US allies and China's concerns of strategic instability." *The Nonproliferation Review*, 2020. https://doi.org/10.1080/10736700.2020.1795368.

Johnson, Dave. "Russia's Conventional Precision Strike Capabilities, Regional Crises, and Nuclear Thresholds." *Livermore Papers on Global Security* no. 3, Livermore, CA: Center for Global Security Research, February 2018. https://cgsr.llnl.gov/content/assets/docs/Precision-Strike-Capabilities-report-v3-7.pdf.

> This Livermore Paper explores nuclear thresholds in Russian military doctrine, particularly how Russian thinking integrates the operational effects of conventional strikes with nuclear deterrence and coercion. Johnson concludes that Moscow views non-nuclear strategic weapons as a means of inflicting unacceptable demage in the early stages of conflict to force enemy capitualition, while still leaving decision-makers nuclear options.

Kreps, Sarah, Jacquelyn Schneider. "Escalation firebreaks in the cyber, conventional, and nuclear domains: moving beyond effects-based logics." *Journal of Cybersecurity* 5, no. 1 (2019). https://doi.org/10.1093/cybsec/tyz007.

> Kreps and Schneider argue that impact of emerging technologies on escalation cannot be explained by the physical effects they create. In particular, they observe that the public perceives cyberattacks as qualitatively different than nuclear or conventional attacks of similar consequences. The individuals exhibit far more caution when it comes to responding aggressively to cyber conflict than either conventional or nuclear. This implies that cyberattacks create a threshold that restrains the escalation of conflict and there is a clear firebreak between cyberspace and either conventional or nuclear domains. The authors underline a need for better understanding which qualities of emerging technology may create new rungs on the escalation ladder and incentivize or de-incentivize states to transition crises toward large-scale armed or nuclear conflict.

5. Impacts on the restoration of deterrence

Core propositions in the literature:

- Multidomain warfare will erode confidence in assured retaliation by increasing the risk of a successful enemy counterforce strike
- Multidomain warfare will encourage greater risk taking to restore confidence in assured retaliation
- Multidomain warfare will increase willingness to keep escalating by a variety of means that may seem less risky than others
- Multidomain warfare does very little to change the calculus of deterrence among large nuclear-armed states armed with robust capabilities

a. On assured nuclear retaliation

Gates, Jonathan. "Is the SSBN Deterrent Vulnerable to Autonomous Drones?" *RUSI Journal* 161, no. 6 (2016): 28–35. https://doi.org/10.1080/03071847.2016.1265834.

Gates argues that some analysts have overstated the anti-submarine warfare potential of autonomous drones. Some emerging technologies, such as magnetic anomaly detectors or very sensitive acoustic detectors, are demonstrating improved capability to detect submerged submarines. Most of these technologies only work at extremely close ranges, and efforts to use unmanned systems to cover wide swaths of open ocean are likely to be frustrated by the propulsion and fuel limitations of existing technologies. Therefore, a submarine underway in the open ocean will continue to enjoy a stealth advantage. Nevertheless, emerging technologies may enhance the capabilities of established anti-submarine warfare forces. They may also prove decisive in chokepoints, such as shallow waters or narrow sea lanes.

See also: Gower, John. "Concerning SSBN Vulnerability." *BASIC (British American Security Information Council)* (blog), June 10, 2016. https://basicint.org/blogs/rear-admiral-john-gower-cb-obe/06/2016/concerning-ssbn-vulnerability---recent-papers/.

Kubiak, Katarzyna. "Quantum technology and submarine near-invulnerability." ELN Global Security Policy Brief, December 2020. https://www.europeanleadershipnetwork.org/wp-content/uploads/2020/12/Quantum-report.pdf.

Geist, Edward and Andrew J. Lohn. "How Might AI Affect the Risk of Nuclear War?" Santa Monica, CA: RAND Corporation, 2018. https://www.rand.org/pubs/perspectives/PE296.html.

Geist and Lohn examine the impact of advanced computing on nuclear security through 2040, describing the types of anticipated concerns and benefits through two illustrative examples: AI for detection and for tracking and targeting and AI as a trusted adviser in escalation decisions. In view of the capabilities that AI may be expected to enable and how adversaries may perceive them, they conclude that AI has the potential to exacerbate emerging challenges to nuclear strategic stability by the year 2040, including by making mobile missile launchers vulnerable to preemption.

Horowitz, Michael C., Paul Scharre, and Alexander Velez-Green. “A Stable Nuclear Future? The Impact of Autonomous Systems and Artificial Intelligence.” Unpublished manuscript, December 2019. https://arxiv.org/abs/1912.05291.

The authors evaluate the relative impact of autonomous systems and artificial intelligence on nuclear stability. They argue that countries may be more likely to use risky forms of autonomy when they fear that their second-strike capabilities will be undermined, and that autonomous nuclear delivery platforms and vehicles could raise the prospect for accidents and miscalculation. They also assess that conventional military applications of autonomous systems could simultaneously influence nuclear force postures and first-strike stability in previously unanticipated ways.

Lieber, Keir A., and Daryl G. Press. “The New Era of Counterforce: Technological Change and the Future of Nuclear Deterrence.” *International security* 41, no. 4 (2017): 9–49. https://www.belfercenter.org/sites/default/files/files/publication/isec_a_00273_LieberPress.pdf.

Lieber and Press posit that two traditional approaches that countries relied on to ensure survivability of strategic forces – that is hiding and protecting the weapons - have been undercut by leaps in weapons accuracy and a revolution in remote sensing. This new era of counterforce then challenges the basis for confidence in contemporary deterrence stability by making the task of securing nuclear arsenals against first strike attack much more challenging.

Loss, Rafael, Joseph Johnson. “Will Artificial Intelligence Imperil Nuclear Deterrence?” *War on the Rocks*, 19 September 2019. https://warontherocks.com/2019/09/will-artificial-intelligence-imperil-nuclear-deterrence/.

Loss and Johnson dispute warnings that AI could erode the fundamental logic of nuclear deterrence by threatening secure second-strike forces. They argue that because of AI’s inherent limitations, splendid counter-force will remain out of reach. While emerging technologies and nuclear force postures might interact to alter the dynamics of strategic competition, AI in itself will not diminish the deterrent value of today’s nuclear forces.

Wilkening, Dean. “Hypersonic Weapons and Strategic Stability.” *Survival* 61, no. 5 (2019): 129-148. https://doi.org/10.1080/00396338.2019.1662125.

Wilkening presents an overview of hypersonic boost-glide and cruise missile technology and discusses implications for crisis and arms race stability. Because they do not follow a predictable flight path in the midcourse phase, hypersonic glide vehicles provide attackers with the capability to quickly destroy a target while evading detection by early warning systems. This also makes defense against glide vehicles difficult. Hypersonic cruise missiles may also enjoy a stealth advantage by flying at altitudes that are opaque to existing sensor systems. As a result, conventionally-armed hypersonic capabilities can pose a new threat to mobile missile forces. States that rely on mobile missiles for nuclear

deterrence may face additional first-strike incentives as a result. In contrast, the U.S. nuclear deterrent does not rely on mobile missile systems. The emergence of hypersonic capabilities may also foment arms racing.

b. On continuity of government

6. Impacts on de-escalation and conflict termination

Core proposition in the literature:

- Multidomain warfare will have an unpredictable effect on de-escalation and war termination.
- Multi-domain warfare may make a negotiated outcome impossible because one party to the conflict has been decapitated through attacks on "continuity of government" capabilities.

Lin, Herbert. "Escalation Dynamics and Conflict Termination in Cyberspace." *Strategic Studies Quarterly* 6, no. 3 (2012): 46-70. https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-06_Issue-3/Lin.pdf.

The author stipulates that even though existing theories of escalation dynamics and conflict termination may serve as useful points of departure, it remains poorly understood today how these theories may apply in cyberspace. In the future, finding ways to manage cyber conflict will be even more intellectually challenging than it was for traditional conflict.

Multi-domain Deterrence and Crisis Management

1. Impacts of new technologies on the ability to assess the adversary's course of action

Core hypotheses in the literature:

- Multidomain complexity erodes crisis stability by undermining such assessments because of improved abilities to act covertly, thereby adding to the risks of crisis instability
- Multidomain complexity will improve confidence in such assessments by making an enemies capabilities and actions more transparent, thereby reinforcing crisis stability

Altmann, Jürgen, and Frank Sauer. "Autonomous Weapon Systems and Strategic Stability." *Survival* 59, no. 5 (2017): 117-42. https://doi.org/10.1080/00396338.2017.1375263.

> Although not yet operational, autonomous weapons systems are likely to emerge in the near future. This development is due to decades of military research and development, the rapidly expanding commercial use of artificial intelligence and robotics, and the accelerating 'spin-in' of commercial technologies into the military realm. Drawing on lessons from the Cold War and the current military use of remotely controlled unmanned systems, Altman and Sauer argue that autonomous weapon systems are prone to proliferation and bound to foment an arms race resulting in increased crisis instability and escalation risks. However, this claim primarily relies on the perceived value that key state actors associated with autonomy. The potential drivers of horizontal proliferation are not considered.

Davis, Zachary S. "Artificial Intelligence on the Battlefield. An Initial Survey of Potential Implications for Deterrence, Stability, and Strategic Surprise." Livermore, CA: Center for Global Security Research, March 2019. https://cgsr.llnl.gov/content/assets/docs/CGSR-AI_BattlefieldWEB.pdf.

> The author explores artificial intelligence's (AI's) implications for national security applications. First, he provides a survey of AI applications for military and strategic operations. Second, potential drawbacks to AI are discussed, which could include the erosion of mutual strategic vulnerability, challenges with AI integration on the battlefield, and other "unknown unknowns" that could result from AI's convergence with other emerging technologies. AI could contribute to intelligence analysis, modelling and simulation, or the development of wargames.

Horowitz, Michael C., Sarah E. Kreps, and Matthew Fuhrmann. "Separating Fact from Fiction in the Debate over Drone Proliferation," *International Security* 41, no. 2 (October 2016): 7–42. https://www.mitpressjournals.org/doi/pdf/10.1162/ISEC_a_00257.

> The authors argue that drone proliferation is unlikely to lead to significant global instability. This line of reasoning stands in contrast to the view the drones are transformative technologies that will uproot global politics. The authors also argue against analysts who view drones as an evolution of existing military capabilities. Instead, they argue that drones' principal advantage lies in the ability to monitor remote areas.

But because drones are vulnerable to air defense systems, they are unlikely to transform international relations between militarily advanced states. As a result, they may be stabilizing in some cases (by allowing states to better understand potential rivals) and destabilizing in others (such as in cases in which the rules of engagement for drones are poorly understood).

National Research Council. *U.S. Air Force Strategic Deterrence Analytic Capabilities: An Assessment of Tools, Methods, and Approaches for the 21st Century Security Environment.* Washington, DC: The National Academies Press, 2014. https://www.nap.edu/catalog/18622/us-air-force-strategic-deterrence-analytic-capabilities-an-assessment-of.

The study's authors were tasked with analyzing the myriad cross domain challenges limiting the U.S. Air Force's ability to deter adversaries and assure allies. The report calls for developing an analytic community to cultivate the necessary intellectual toolkit for personnel to prepare for a rapidly changing security environment, including the prospect of deep uncertainty. Training a corps of analysts who are knowledgeable in emerging technologies is necessary to grapple with complexity and provide leaders with sound advice on the battle field of the future and managing nuclear deterrence and assurance. Emerging technologies play a central role in a new conceptual framework to assess an adversary's intentions in an era characterized by complexity.

Rovner, Joshua. "Give Instability a Chance?" *War on the Rocks*. July 28, 2020. https://warontherocks.com/2020/07/give-instability-a-chance/.

Rovner considers the argument that there may be strategic benefits to the crisis instability created by new intelligence, surveillance and reconnaissance capabilities. Such technologies could provide possessors with a potential first strike advantage. Rovner discusses the competing views that this instability is either helpful or hurtful for deterrence. Advocates of "optimum instability" argue that potential aggressors may be more deterred if they fear the possibility, however remote, that they could suffer a disarming first strike. Rovner concedes the logic of this argument but argues that there are several practical challenges to a policy of optimum instability.

2. Impacts on the ability to consult and deliberate

Core hypotheses in the literature:

- Multidomain complexity robs the consultative process of time and clarity
- Multidomain complexity drives increased reliance on autonomous systems, reducing human control.

Hersman, Rebecca, et al. "Under the Nuclear Shadow: Situational Awareness Technology and Crisis Decisionmaking." Washington, DC: Center for Strategic and International Studies, March 18, 2020. https://ontheradar.csis.org/analysis/final-report/.

The authors find that the chance of conflict or crises between nuclear armed states is increasing due to the shared reliance of nuclear and conventional forces on common

situation awareness systems. Emerging situational awareness technology could further influence nuclear decision making. The authors identify three escalation pathways that result from the current and emerging set of situational awareness capabilities: provocation, entanglement, and information complexity. Nuclear decision makers, they argue, must assess the risks and benefit of complex situational awareness technologies to better avoid the risk of biased decision making. To do so, new perspectives on information dominance are needed.

See also: Hersman, Rebecca, "Wormhole escalation in the new nuclear age," *Texas National Security Review*, Summer 2020. https://tnsr.org/2020/07/wormhole-escalation-in-the-new-nuclear-age/

Johnson, James. "Delegating strategic decision-making to machines: Dr. Strangelove Redux?" *Journal of Strategic Studies* (2020): 1-39. DOI: 10.1080/01402390.2020.1759038.

Johnson analyzes the impact of strategic stability of the use of artificial intelligence (AI) in the strategic decision-making process, in particular, the risks and trade-offs of pre-delegating military force (or automating escalation) to machines. The author echoes the concerns of other analysts that AI-enabled decision making can lead to undesirable outcomes. However, Johnson argues that the risks of delegating decision making to AI are not that AI systems might make decisions based on hidden biases or bad logic, but rather that AI may induce overconfidence in response in situations that would be better managed with caution and prudence. Implementing AI into early warning systems may fail in periods of crisis instability when cyberattacks, for instance, precipitate systemic failure that could magnify the conditions leading to inadvertent escalation.

Technology for Global Security, Preventive Defense Project, Stanford University, Nautilus Institute, N2 Collaborative. "Social Media Storms And Nuclear Early Warning Systems. A Deep Dive and Speed Scenarios Workshop." January 8, 2019. https://securityandtechnology.org/wp-content/uploads/2020/07/social_media_nuclear_war_synthesis_t4gs_report.pdf.

Social media's ability to drastically accelerate communication poses a unique challenge to managing Nuclear Command, Control and Communication (NC3) in crises. The authors analyzes four case studies, primarily in Asia, to assess how social media amplifies tensions that threatens to boil over into nuclear weapons use. Across each scenario, the authors called for creating circuit breakers to intentionally slow escalatory spirals that social media amplifies. Hot lines, shared sensor data, market and third-party communication channels, all can provide policy makers with timely information that prevents social media from corrupting rational thought in determining the use of nuclear weapons. Although the task is significant, all parties from policy makers to social media users can play an important role in preventing social media's pace from fueling escalation amidst crises.

Unal, Beyza and Patricia Lewis. "Cybersecurity of Nuclear Weapons Systems Threats, Vulnerabilities and Consequences." London, UK: Chatham House, January 2018. https://www.chathamhouse.org/sites/default/files/publications/research/2018-01-11-cybersecurity-nuclear-weapons-unal-lewis-final.pdf.

> The authors assess the cyber risks and vulnerabilities associated with nuclear weapons, the current state of offensive cyber activities against nuclear weapons, and provide recommendations towards improving resilience. Challenges arise because nuclear weapon systems were developed before many of these digital vulnerabilities because apparent. Cyber risks are different in peacetime and during times of heightened tensions. Nuclear weapon states are responsible for ensuring the resiliency of their nuclear weapons, but input from academia and civil society should be encouraged. The authors mention that if a command and control system has been compromised, it will not be trusted for decision making, which could affect the ability to consult and deliberate.

3. Impacts on signaling to adversaries and allies

Core propositions in the literature:

- Multidomain complexity adds to the fog of war, complicating messaging
- Multidomain complexity can improve signaling by allowing more direct channels
- Multidomain dominance by one actor over another creates strong one-way messaging opportunities

Green, Brendan R., and Austin Long. "Invisible Doomsday Machines: The Challenge of Clandestine Capabilities and Deterrence." *War on the Rocks*, December 15, 2017. https://warontherocks.com/2017/12/invisible-doomsday-machines-challenge-clandestine-capabilities-deterrence/.

> The authors discuss how clandestine military capabilities may be used for political military objectives, such as deterrence. Secrecy and surprise are assets for any military operation, but the utility of clandestine capabilities is significantly degraded when revealed. As a result, clandestine capabilities are often compartmentalized, and those with full knowledge of such systems are small. To decide whether to reveal or conceal a capability in support of deterrence strategies, policy makers should consider its uniqueness and whether or not it provides opportunities for deception.
>
> See also: Long, Austin, and Brendan R. Green. "Stalking the secure second strike." *Journal of Strategic Studies*, 38:1 (2015): 38-73. https://doi.org/10.1080/01402390.2014.958150.

Meserole, Chris. "Artificial Intelligence and the Security Dilemma." Brookings (blog), November 6, 2018. https://www.brookings.edu/blog/order-from-chaos/2018/11/06/artificial-intelligence-and-the-security-dilemma/.

> Meserole contends that the uncertainty surrounding AI may intensify security dilemmas between rivals, potentially precipitatingan AI arms race or the outbreak of war. Although technical advances occur rapidly and could precipitate an escalation spiral, there are

avenues for cooperation between the United States and China to prevent issues of uncertainty or complexity from stoking escalation. Meserole finds that partial cooperation and competition offers the best solution to head off an AI arms race while also opening channels of communication between the two states. An AI arms race will exacerbate the brewing security dilemma between the United States and China, and action is necessary to forestall the consequences of technological uncertainty.

Montgomery, Evan Braden. "Signals of strength: Capability demonstrations and perceptions of military power." *Journal of Strategic Studies* 43, no.2 (2020): 309-330 https://doi.org/10.1080/01402390.2019.1626724.

States have historically relied on capability demonstrations to deter and assure, reaping political benefits from signaling strength. Today's technological arms race increases incentives for states to demonstrate capabilities of emerging technologies. The uncertainty and opacity of virtual emerging technologies elude the traditional rationale for demonstration by demanding secrecy lest technology weaken the intended effects. Demonstrations of physical emerging technologies such as hypersonic missiles or robotics, on the other hand, can signal technological achievement without surrendering secret operational or technological data. The benefits of deterring, assuring, or imposing costs by signaling may not accrue as directly as in the past once emerging technologies replace traditional weapons systems.

Zegart, Amy. "Cheap fights, credible threats: The future of armed drones and coercion." *Journal of Strategic Studies* (2018): 6-46. https://doi.org/10.1080/01402390.2018.1439747.

The author argues that armed drones could be used as a coercive signaling tool by a state with advanced drone technology against another without it. This is contrary to preexisting conclusions on the coercive use of armed drones, because drones are inherently cheaper than other forms of intervention. Based on survey results from senior foreign military officers, the author finds that drones may be as credible as ground troops in signaling because it is more likely that armed drone operations could be sustained for periods of time.

Wong, Yuna Huh, et al. *Deterrence in the Age of Thinking Machines*. Santa Monica, CA: RAND Corporation, 2020. https://www.rand.org/content/dam/rand/pubs/research_reports/RR2700/RR2797/RAND_RR2797.pdf.

The report presents the results of a wargame exploring the impact of AI and autonomous systems on deterrence and escalation in a hypothetical future conflict scenario involving the United States, China, Japan, South Korea, and North Korea. The wargame resulted in several interesting outcomes. In the game, manned systems had a stronger deterrent effect than unmanned systems, as the stakes of attacking manned systems were seen as higher. In addition, greater reliance on unmanned systems at the expense of human troops was not seen by U.S. allies as a signal a reduced security commitment. Rather, they were seen as more capable and more likely to be deployed in

combat. Delegating control to autonomous systems was used to signal resolve to the adversary. Finally, greater reliance on autonomous systems resulted in both deliberate and inadvertent escalation.

4. Impacts on the ability to integrate operations for strategic effect

Core propositions in the literature:

- Multidomain competition strengthens the capability for integration by advanced states
- Multidomain competition favors those with advanced command-and-control systems enabling all-domain operations
- Multidomain competition erodes the ability to dominate

Boulanin, Vincent, et al. *Artificial Intelligence, Strategic Stability and Nuclear Risk*. Solna, Sweden: Stockholm International Peace Research Institute, June 2020. https://www.sipri.org/sites/default/files/2020-06/artificial_intelligence_strategic_stability_and_nuclear_risk.pdf.

An AI renaissance, the authors of this report contend, enabled a series of technological advances that signal how the rapid implementation of AI across weapons systems can damage strategic stability. The boundaries of AI's impact on strategic and conventional weapons has not yet reached maturity, and will not for quite some time. In spite of this, current technological advancements convince the authors that risk of inadvertent escalation will only increase when AI is operationalized in nuclear weapons systems. The report concludes with a call for a return to arms control agreements for negotiation between states, confidence building measures, collaboration on universal AI applications, and agreement among nuclear armed states for the limited employment of AI in their nuclear weapons systems.

Clark, Brian, Daniel Pratt and Harrison Schramm. "Mosaic Warfare: Exploiting Artificial Intelligence and Autonomous Systems to Implement Decision-Centric Operations." Washington, DC: Center for Strategic and Budgetary Assessments, 2020. https://csbaonline.org/research/publications/mosaic-warfare-exploiting-artificial-intelligence-and-autonomous-systems-to-implement-decision-centric-operations/publication/1.

The authors argue that despite ongoing efforts to realign U.S. defense posture and better integrate capabilities across domains, the U.S. military may be unable to gain and maintain superiority over its great power competitors by simply using improved versions of today's forces. Instead, a new warfighting approach is needed that uses artificial intelligence and autonomous systems as the foundation of a decision-centric warfare that enables faster and more effective decisions. AI and autonomous systems can greatly increase adaptability for U.S. forces and create complexity or uncertainty for the enemy. Since the next major arena of military competition could be information and decision-making, the U.S. military could establish a prolonged advantage by harnessing emerging technologies for AI and autonomous systems.

Futter, Andrew. "The Risks Posed by Emerging Technologies to Nuclear Deterrence." In *Perspectives on Nuclear Deterrence in the 21st Century*, edited by Unal, Beyza, et al. London, UK: Chatham House, April 2020. https://www.chathamhouse.org/sites/default/files/2020-04-20-nuclear-deterrence-unal-et-al.pdf.

> Of all the technologies listed as "emerging", the author assesses that the two main technologies that could challenge nuclear deterrence are sensing technologies and artificial intelligence. The author notes that while new technologies have been introduced into nuclear weapon systems, such as stealth aircraft and cruise missiles, these have reinforced rather than upset the status quo. In contrast, newer emerging technologies may augment or replace functions typically reserved for nuclear weapons. Integrating new technologies may bring new challenges, stating that "it is much harder to assess or quantify the threat posed by intangible computer code than it is for a large and conspicuous nuclear-armed ballistic missile."

Space Strategy at a Crossroads: Opportunities and Challenges for 21st Century Competition. Edited by Benjamin Bahney. Livermore, CA: Center for Global Security Research, May 2020. https://cgsr.llnl.gov/content/assets/docs/space-strategy-at-a-crossroads.pdf

> This edited volume contains contributions from various strategic thinkers on the role of space in the U.S. national defense strategy, existing strategies for war in space and space in war, and necessary partnerships for managing long-term strategic competition. The contributors identify challenges to integrating space defense into existing deterrence strategies and way to involve the U.S. space force and other stakeholders, such as the scientific research community and allies, in these goals. This will require moving past historical silos in different domains and embracing both top-down and bottom-up approaches for creating and operationalizing strategies.

Multi-domain Competition and Peacetime Rivalry

1. Impacts on the ability to gain new advantages of political or military consequence

Core propositions in the literature:

- Multidomain competition creates a potential for significant new strategic military advantages for those first to master the needed doctrinal and operational innovations
- Multidomain competition favor those capable of managing complexity
- Multidomain competition creates advantages that are likely to prove short-lived
- Multidomain competition will encourage competition in complex and poorly understood technologies, thereby eroding arms race stability

Abercrombie, Clarence; and Heather Venable. "Muting the Hype over Hypersonics: The Offense-Defense Balance in Historical Perspective." *War on the Rocks*. May 28, 2019. https://warontherocks.com/2019/05/muting-the-hype-over-hypersonics-the-offense-defensebalance-in-historical-perspective/.

> The authors argue that arms races will always oscillate between the dominance of offensive and defensive capabilities and hypersonic weapons are no exception. The dominance of offensive capabilities can emphasize the deterrent effect of mutually assured destruction and stabilize global security. While there is currently no effective defense against hypersonic weapons, history suggests that defenses will inevitably emerge—one such option is the potential for directed energy defenses. On the offensive side, a stable balance of power requires some degree of parity in hypersonic capabilities.

Horowitz, Michael C., Gregory C. Allen, Edoardo Saravalle, Anthony Cho, Kara Frederick, and Paul Scharre. "Artificial Intelligence and International Security." Washington, DC: Center for a New American Security, July 2018. https://www.cnas.org/publications/reports/artificial-intelligence-and-international-security.

> The authors examine the potential consequences of advances in artificial intelligence for the national security community. Nearly every aspect of national security could be transformed by artificial intelligence. AI has applications for defense, intelligence, homeland security, diplomacy, surveillance, cybersecurity, information, and economic tools of statecraft. The authors argue that AI is not clearly positive or disruptive. There are many areas where the United States and its allies would benefit from a wider application of AI, but there are areas where restraints are needed to restrict the disruptive effects of this technology.

Kania, Elsa B. "Chinese Military Innovation in the AI Revolution." *The RUSI Journal* 164, no. 5-6: 26-34. https://www.tandfonline.com/doi/abs/10.1080/03071847.2019.1693803. DOI: 10.1080/03071847.2019.1693803.

> The Chinese People's Liberation Army (PLA) anticipates that today's advances in emerging technologies, particularly AI, could catalyze a new military revolution. The PLA's capacity to operationalize AI for national defense will be shaped and possibly

constrained by the challenges of military big data. The PLA is concerned with improving its collection, management and processing of data. Success in intelligentized warfare will depend upon building up a high-quality pool of military data, an integral foundation for intelligent command and control. If successful, the PLA could succeed in realizing its aspirations of becoming a world-class military, changing the balance of power in the Indo-Pacific and beyond.

Kallenborn, Zachary, and Philipp C. Bleek. “Swarming Destruction: Drone Swarms and Chemical, Biological, Radiological, and Nuclear Weapons.” *The Nonproliferation Review* 25, no. 5–6 (September 2, 2018): 523–43. https://doi.org/10.1080/10736700.2018.1546902.

Drone swarms are multiple unmanned systems capable of coordinating their actions to accomplish shared objectives. These swarms have major implications for the future of warfare. One important set of implications relates to the ability of drone swarms to complement, challenge, and even substitute for chemical, biological, radiological, and nuclear (CBRN) weapons. Swarming drones might enable more effective CBRN delivery, they might facilitate standoff detection, or otherwise impede an adversary’s ability to threaten or employ CBRN weapons. At the same time, many CBRN-relevant applications of this technology entail significant technical challenges even for very sophisticated states, so uncertainty remains around whether, how much, and when drone-swarm technology will complement, challenge, or substitute for CBRN weapons.

Kania, Elsa B. and John K. Costello, "Quantum technologies, U.S.-China strategic competition, and future dynamics of cyber stability," 2017 International Conference on Cyber Conflict (CyCon U.S.), Washington, DC, 2017, pp. 89-96, doi: 10.1109/CYCONUS.2017.8167502.

The current realities of the cyber domain could be radically disrupted by the advent of quantum communications and quantum computing. The consequent challenges for future cyber security and strategy require a nuanced analysis of these technologies and their likely employment by major powers. These quantum technologies could advantage defense and offense in the cyber domain. While the “shield” enabled by quantum communications would contribute to technological deterrence through denial, the asymmetries of vulnerability that might result could potentially undermine military cyber stability, while exacerbating the risks of misperception through complicating intelligence collection. The strategic impact of these disruptive technologies will depend upon the approaches of great powers, particularly the United States and China.

Lindsay, Jon R. and Gartzke, Erik. “Politics by many other means: The comparative strategic advantages of operational domains.” *Journal of Strategic Studies*, 2020. https://doi.org/10.1080/01402390.2020.1768372

The land, sea, air, space, and cyber domains have distinct operational characteristics. Specialization in the means of using or threatening force is not just a technical issue because choices to use different kinds of military instruments have political consequences. Conventional and nuclear capabilities in these domains have comparative advantages and disadvantages for three general types of strategy – coercion, warfighting,

and deception. More complex strategies that cross or combine domains may achieve force-multiplying synergies or create significant trade-offs that affect military and political performance. This article describes the strategic constraints and opportunities posed by specialized force structures.

Volpe, Tristan A. "Dual-use distinguishability: How 3D-printing shapes the security dilemma for nuclear programs." *Journal of Strategic Studies* 42, no. 6 (2019): 814-840. https://doi.org/10.1080/01402390.2019.1627210.

Additive manufacturing is being adopted by nuclear programs to improve production capabilities, yet its impact on strategic stability remains unclear. The author uses the security dilemma to assess incentives for arms racing as the emerging technology becomes integrated into nuclear supply chains. Innovations sow the ground for competition by making it easier to produce weapons and harder to distinguish civil from military motives. But additive manufacturing could still mature into an asset by revealing greater information about nuclear aspirants. Beyond the nuclear realm, the article refines offense-defense theory to explain how changes in non-military technology shape the practice of deception.

2. Impacts on the willingness to commit to mutual restraint

Core propositions in the literature:

- Multidomain competition decreases the willingness because of the competitive advantages still to be gained
- Multidomain competition ultimately increases the willingness to restrain because mutual vulnerability is inescapable
- Multidomain competition burdens arms control with the need to adapt to remain relevant to strategic stability and risk reduction.

Gompert, David C., and Phillip C. Saunders. "Sino-American Strategic Restraint in an Age of Vulnerability." *Strategic Forum* (January 2012). http://ndupress.ndu.edu/Portals/68/Documents/stratforum/SF-273.pdf.

Gompert and Saunders note that despite their vast power, the United States and China are becoming increasingly and mutually vulnerable in three key strategic domains: nuclear, space and cyber. Due to the dim arms control prospects, both powers are likely to develop stronger offensive capabilities to deter the other side. The authors suggest that negotiations on mutual restraint could start with no-first use pledges in the nuclear, antisatellite and cyber domains.

Lewis, James A. "Emerging Technologies and Next Generation Arms Control." Washington, DC: Center for Strategic and International Studies, October 21, 2019. https://www.csis.org/analysis/emerging-technologies-and-next-generation-arms-control.

The author argues that Cold War arms control agreements face two dilemmas: first, they do not cover the emerging technologies that will build the next generation of weapons,

and second, China is not a party to most of them. Emerging technologies change the equation for stability and deterrence in ways we cannot easily predict. These technologies make Cold War agreements—if they even apply—less useful. U.S. relations with Russia and China are too parlous to begin a new generation of arms control talks for emerging technologies, but as arsenals accumulate and as the risk from emerging weapons technologies grows, this will change. Discussions of the implications of these technologies for stability could form a new agenda for arms control.

Marchisio, Sergio. "The Final Frontier: Prospects for Arms Control in Outer Space." Global Security Policy Brief, European Leadership Network, July 2019. https://www.europeanleadershipnetwork.org/policy-brief/the-final-frontier-prospects-for-arms-control-in-outer-space/.

This ELN report argues that more than ever, a set of international norms addressing the security of outer space activities is needed. It is imperative to create a platform for exchanging views on the establishment of general principles of responsible behavior, transparency and confidence building measures and make workable recommendations. These should address challenges associated with the dual-use applications, civil and military, of outer space objects and capabilities, but should avoid hindering access to such technologies for peaceful purposes. In this regard, regional organizations have an important role to play to advance normative instruments, such as codes of conduct.

Maas, Matthijs M. " How viable is international arms control for military artificial intelligence? Three lessons from nuclear weapons." *Contemporary Security Policy* 40, no. 3 (2019): 285-311. https://doi.org/10.1080/13523260.2019.1576464.

The author compares establishing viable arms control regimes for military AI with regulating nuclear weapons, specifically to map out opportunities and potential challenges in the AI domain. Deployed militarized AI systems are likely to suffer from operational safety limitations, which gives rise to ethical and legal concerns about potential accidents. Maas argues that "meaningful human control" will not reduce the rate of "normal accidents," rendering this an ineffectual concept for AI governance. Instead, there is hope for domestic political groups to provide arms control concepts, or for subject matter experts to prevent or affect a nascent AI arms race.

Morgan, Forrest E. "Military Applications of Artificial Intelligence. Ethical Concerns in an Uncertain World." Santa Monica, CA: RAND Corporation, 2020. https://www.rand.org/content/dam/rand/pubs/research_reports/RR3100/RR3139-1/RAND_RR3139-1.pdf.

According to this RAND report, the application of AI in war raises new and complex ethical questions regarding its role vis-à-vis the role of human warfighters. Such questions include whether AI systems can comply with humanitarian principles, whether they will be sufficiently reliable and predictable, and what effects they will have on escalation and stability. The authors recommended for the U.S. to follow discussions at the UN and track the evolving positions held by stakeholders; seek greater technical

cooperation and policy alignment with allies and partners regarding the development and employment of military AI; and explore confidence-building and risk-reduction measures with China, Russia, and other states attempting to develop military AI.

Persi Paoli, Giacomo, Kerstin Vignard, David Danks, Paul Meyer. "Modernizing Arms Control: Exploring responses to the use of AI in military decision-making." Geneva, Switzerland: UNIDIR, August 2020. https://unidir.org/publication/modernizing-arms-control.

This UNIDIR report focuses on the use of AI-enabled decision support systems by militaries. Although many of the traditional tools of arms control remain relevant, new ways of working and new relationships will be necessary to address these challenges effectively. The traditional arms control toolbox will not become obsolete if the arms control community is open and willing to embrace new forms of collaboration as well as adapt traditional ones to fully leverage the know-how of the scientific expert community, most of which now resides in the private sector. There is no "one stop" solution, a web of responses and incentive structures will be needed. While governments remain the natural owners of traditional arms control tools, possible measures do not always require government leadership, industry has its own responsibilities.

Williams, Heather. "Asymmetric arms control and strategic stability: Scenarios for limiting hypersonic glide vehicles." *Journal of Strategic Studies* 42, no. 6 (2019): 789-813. https://doi.org/10.1080/01402390.2019.1627521.

Williams concludes that for a long time there was a clear gap between the strategic stability concepts of the United States and Russia. While the United States defined strategic stability with a focus on maintaining a survivable second-strike capability, Russia considered non-nuclear forces and the balance of offense-defense essential to strategic stability. The future of arms control will depend on how the two sides manage to bridge these differences. This will probably require a new asymmetric framework that incorporates missile defense, advanced conventional capabilities, emerging technologies and non-strategic nuclear weapons.

3. Impacts on the ability to verify treaty compliance

Core propositions in the literature:

- Multidomain competition enhances the ability to verify by adding transparency
- Multidomain competition erodes the ability to verifiy by expanding the space for covert operations

Chyba, Christopher F. "New Technologies & Strategic Stability." *Daedalus* 149, no. 2 (2020): 150-170. https://doi.org/10.1162./daed_a_01795.

A variety of new technologies, ranging from broad enabling technologies to specific weapon systems, may threaten or enhance strategic stability. Formal arms control to contain dangers posed by some of these seems technically possible, though currently politically difficult to achieve. Others, particularly enabling technologies, resist arms

control based on effective verification. And in any case, such verification may, at this time, be politically difficult. The major powers will therefore instead have to find other ways to cope with these technologies and their implications. These options should include exchanges with potential adversaries so that pathways to nuclear escalation, and possible mitigating steps, can be identified and discussed.

Geist, Edward. "It's Already Too Late to Stop the AI Arms Race—We Must Manage It Instead." *Bulletin of the Atomic Scientists* 72, no. 5 (2016): 318 –321. https://doi.org/10.1080/00963402.2016.1216672.

While an ongoing campaign argues that an agreement to ban autonomous weapons can forestall AI from becoming the next domain of military competition, Geist suggests that an AI arms race is already here. He draws on the history of AI weaponization and arms control for other technologies to argue that AI and robotics researchers should cultivate a security culture to help manage the AI arms race. By monitoring ongoing developments in AI weapons technology and building the basis for informal "Track II" diplomacy, AI practitioners could begin building the foundation for future arms-control agreements.

Philippe, Sebastien, Alexander Glaser, and Edward W.Felten, "A cryptographic escrow for treaty declarations and step-by-step verification." *Science & Global Security* 27, no. 1 (2019): 3-14. https://doi.org/10.1080/08929882.2019.1573483.

The verification of arms-control and disarmament agreements requires states to provide declarations, including information on sensitive military sites and assets. There are cases, however, in which negotiations of these agreements are impeded as states are reluctant to provide any such data, because of concerns about prematurely handing over militarily significant information. This article presents a cryptographic escrow that allows a state to make a complete declaration of sites and assets at the outset and commit to its content, but only reveal the sensitive information therein sequentially. Combined with an inspection regime, this escrow allows for step-by-step verification of the correctness and completeness of the initial declaration so that the information release and inspections keep pace with parallel diplomatic and political processes.

Patton, Tamara & Glaser, Alexander. "Deferred verification: the role of new verification technologies and approaches." *The Nonproliferation Review* 26, no. 3-4 (2019): 219-230. https://doi.org/10.1080/10736700.2019.1629072.

Researchers have recently proposed a new approach to nuclear arms control verification, called "deferred verification." The concept forgoes inspections at sensitive nuclear sites and of nuclear weapons or components in classified form. A state first divides its nuclear program into a closed segment and an open segment. The total fissile-material inventory in the closed segment, which includes the weapon complex, is known and declared with very high accuracy. Essentially no inspections take place in the closed segment. In contrast, inspectors have access to the open segment, which includes in particular the civilian nuclear sector. Deferred verification relies primarily on established safeguards techniques and avoids many unresolved verification challenges, such as the need for information barriers for warhead confirmation measurements.

4. Impacts on alliances and coalitions

Core propositions in the literature:

- Multidomain competition will amplify pre-existing problems related to the stratification of alliances between/among the more and less capable of multidomain situational awareness
- Multidomain competition will galvanize innovation in alliances long reluctant to embrace major changes to their deterrence postures
- Multidomain competition will strengthen extended deterrence by enhancing the military potential of advanced countries
- Multidomain competition will weaken assurance of allies who fear being left behind or pawns in an escalating but non-nuclear conflict

Gilli, Andrea. "NATO-Mation": Strategies for Leading in the Age of Artificial Intelligence," *NDC Research Paper* 15. Rome: NATO Defense College, December 2020. https://www.ndc.nato.int/download/downloads.php?icode=671.

> The author argues that NATO cannot be a bystander during a technological transformation driven by artificial intelligence, machine learning and big data. In order to preserve their military and technological leadership in the near future, NATO allies have to integrate AI both at the national and coalition level. This will bring massive challenges. Gilli advances a number of proposals centered on the concept of "NATO-mation" aimed at equipping the Alliance with the capabilities, organizational structures and strategies to compete in a world of AI-enabled militaries. The discussion on the "NATO-mation" is divided into 11 building blocks, including ethical purpose; innovation; technological superiority; arms control and technology regimes; and primacy of democracy.

Lin-Greenberg, Erik. "Allies and Artificial Intelligence: Obstacles to Operations and Decision-Making." *Texas National Security Review* 3, no. 2, (2020): 56-76. https://tnsr.org/2020/03/allies-and-artificial-intelligence-obstacles-to-operations-and-decision-making/.

> The paper stipulates that AI poses unique challenges to multinational military operations and decision-making that need to be further explored. In particular, the data- and resource-intensive nature of AI development creates barriers to burden-sharing and interoperability that can hamper multinational operations. Also, by accelerating the speed of combat and providing adversaries with a tool to heighten mistrust between allies, AI can strain the complex processes that allies and security partners use to make decisions.

Mehta, Rupal N. "Extended deterrence and assurance in an emerging technology environment." *Journal of Strategic Studies* (2019): 1-25. DOI: 10.1080/01402390.2019.1621173.

> The paper explores an impact of emerging technologies on extended deterrence commitments and assurance of allies. Mehta argues that while new technologies such as

drones and hypersonic glide vehicles may enhance the ability to deter potential adversaries, allies may be less assured by these new capabilities.

Tonin, Matej. "Artificial Intelligence: Implications For Nato's Armed Forces." NATO Parliamentary Assembly, Science and Technology Committee (STC), Sub-Committee on Technology Trends and Security (STCTTS), 13 October 2019. https://www.nato-pa.int/download-file?filename=%2Fsites%2Fdefault%2Ffiles%2F2019-10%2FREPORT%20149%20STCTTS%2019%20E%20rev.%201%20fin-%20ARTIFICIAL%20INTELLIGENCE.pdf.

The report provides a broad overview of opportunities, non-technical and technical challenges and uncertainities related to the AI impact on NATO armed forces and at the strategic lelvel. Ultimately, the author observes that it is too early to tell what the effects of AI in the military and strategic affairs will be, in part because of decisions states have yet to make. What remains almost certain, however, is that the adoption of AI will have an impact across the full spectrum of force, as well as all other defence tasks, given AI's omni-use aspect.

Additional Readings:

Brose, Chris. *The Kill Chain*: *Defending America in the Future of High-Tech Warfare.* New York: Hachette Books, 2020.

Futter, Andrew. *Hacking the Bomb: Cyber Threats and Nuclear Weapons.* Washington, DC: Georgetown University Press, 2018.

Lieber, Keir A., Daryll Press, *The Myth of the Nuclear Revolution: Power Politics in the Atomic Age*. Ithaca and London: Cornell University Press, 2020.

Posen, Barry R. *Inadvertent Escalation: Conventional War and Nuclear Risks.* Ithaca and London: Cornell University Press, 1991.

Sanger, David. *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*. New York: Penguin Random House, 2018.

Singer, Peter, August Cole. *Ghost Fleet: A Novel of the Next World War*. New York: An Eamon Dolan Book, 2016.

Scharre, Paul. *Army of None: Autonomous Weapons and the Future of War*. New York: W.W.Norton &Company, 2018.

Cross-Domain Deterrence: Strategy in an Era of Complexity, edited by Erik Gartzke and Jon R. Lindsay. New York, NY: Oxford University Press, 2019.

Strategic Latency: Red, White, and Blue: Managing the National and International Security Consequences of Disruptive Technologies, edited by Zachary S. Davis and Michael Nacht. Livermore: Center for Global Security Research, Lawrence Livermore National Laboratory, February 2018.

Three Tweets to Midnight: Effects of the Global Information Ecosystem on the Risk of Nuclear Conflict, edited by Harold A. Trinkunas, Herbert Lin, Benjamin Loehrke. Stanford, California: Hoover Institution Press, 2020.

Center for Global Security Research
Lawrence Livermore National Laboratory
P.O. Box 808, L-189 Livermore, California 94551
https://CGSR.llnl.gov

This work was performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract DE-AC52-07NA27344. LLNL-TR-819882