Invited Perspective: Anticipating the Effects of Emerging Technologies on Nuclear Deterrence

NOVEMBER 2021

STRATEGIC MULTILAYER ASSESSMENT

Author: Melanie Sisson, Brookings Institution

Series Editor: Sarah Canna, NSI

Melanie W. Sisson, Brookings Institution

Melanie W. Sisson is a fellow in the Brookings Institution Foreign Policy program's Center for Security, Strategy, and Technology where she researches the use of the armed forces in international politics, U.S. national security strategy, and military applications of emerging technologies. Sisson previously was vice president of analysis at Govini, an early-stage national security AI/ML technology company, and senior fellow and director of the Stimson Center Defense Strategy and Planning program. At Stimson, Sisson partnered with the Stanley Center and U.N. Office of Disarmament Affairs to address the implications for international security of military applications of AI, and published "Military Coercion and US Foreign Policy: The Use of Force Short of War" (Routledge, 2020). A former senior national security project associate with the RAND Corporation, manager of program evaluation for a non-profit mental health organization, and member of the U.S. intelligence community, Sisson earned a doctorate in political science from the University of Colorado at Boulder, and a master's from the Columbia University School of International Affairs. She is a consultant to the U.S. Department of Defense, lectures regularly with universities nationwide, and is published in national media outlets and academic journals.

Invited Perspective: Anticipating the Effects of Emerging Technologies on Nuclear Deterrence

Melanie W. Sisson, Brookings Institution[1]

The effectiveness of nuclear deterrence depends upon mutual confidence in second-strike capabilities - for nuclear deterrence to work, nuclear-armed competitors must all believe that each can absorb a first strike and still return a nuclear response. Emerging technologies being pursued by US competitors that enhance their ability to locate, track, and target nuclear assets, and those that can be used to compromise or to damage components of nuclear communication, command, and control (NC3) erode second-strike and put at risk the future deterrent effectiveness of US strategic forces. The United States can guard against this outcome by modernizing its air- and sea-based nuclear assets, developing resilient and redundant cyber defenses, and actively pursuing international agreements that limit the deleterious effects of ISR and that prohibit kinetic or cyber attacks on terrestrial and satellite-based components of NC3.

Today's geopolitical landscape is crowded with unsteadying influences. The COVID-19 pandemic introduced an acute shock into an environment already unsettled by extreme weather events, socio-economic dislocation, resurgent nationalisms, China's economic and military rise, Russia's regroup, and rapid advances in disruptive technologies. To acknowledge that much is changing, however, is not to overlook that some things stay the same. Indeed, although advances in modern technologies create new pressures to reinforce the foundations of nuclear stability developed during the Cold War, they do not up-end them.

The effectiveness of nuclear deterrence today remains dependent upon ensuring mutual confidence in second-strike capabilities - for nuclear deterrence to work, nuclear-armed competitors must all believe that each can absorb a first strike and still return a nuclear response.[2] In many cases, emerging technologies are being pursued for purposes other than negating second-strike capability, and for now many of their applications remain more planned than realized. Nonetheless, their potential independently or in conjunction with other technologies to erode second-strike, and the possibility that they will be deployed, generate justifiable concern about the future deterrent effectiveness of US strategic forces.

[1] *Contact Information*: MSisson@brookings.edu

[2] The ability of a state to return any nuclear weapon onto the territory of another state is here considered "second-strike sufficiency."

US defense strategy seeks to deter attacks on the United States and its allies by maintaining an effective strategic nuclear arsenal and by demonstrating conventional warfighting superiority. While the credibility of the US nuclear arsenal is not in question, there is concern within the Department of Defense and elsewhere in the national security community about the extent to which conventional US forces are adequately modern and ready. These insecurities mean that the United States is unlikely to forgo acquisition of emerging and disruptive technologies (EDTs), many of which cross the boundary between conventional and nuclear application. The United States should expect competitors to do the same and can anticipate that those that are nuclear-armed will recognize, and seek ways to counter, the effects dual-use technologies might have on the utility of their own nuclear assets.

Russia does not need to grow its numbers of warheads or delivery vehicles, but there are domestic, regional, and global dynamics that make hypersonic missiles, artificial-intelligence (AI)-enabled intelligence, surveillance, and reconnaissance (ISR) capabilities, and AI-enabled cyber operations appealing.[3] China, by comparison, does have reason to seek to expand its arsenal and extend its dispersal and to bolster its offensive and defensive cyber capabilities, as well as regionally-driven reasons to pursue hypersonic missiles. Although unable to reach anything near nuclear parity with the United States, North Korea and Iran might pursue hypersonic capabilities to heighten risk to their neighbors and have evidenced the ability to deploy disruptive and potentially destructive cyber weapons that could constitute a threat to NC3.[4]

The United States nuclear deterrent remains robust to China's numeric expansion and to competitor hypersonic delivery systems.[5] Sophisticated AI-enabled cyber threats and the combination of advanced sensing, AI, and unhumanned platforms into systems useful for ISR, however, do have direct potential to degrade the timeliness and potency of US second-strike. The United States can guard against these undesirable outcomes by modernizing its air- and sea-based nuclear assets, developing resilient and redundant cyber defenses, and actively pursuing international agreements that limit the deleterious effects of ISR and that prohibit kinetic or cyber attacks on terrestrial and satellite-based components of NC3.

---

[3] Russia has a declared stock of 1,326 strategic warheads deployed on 485 ICBMs. Credible estimates place the total number of Russia's strategic, non-strategic, and retired warheads at close to 10,000. See: SIPRI Yearbook, 2020. AI here includes narrow applications and machine learning/deep learning, but excludes general artificial intelligence – the category used to refer to fully intellectually realized, sentient AI. For a disaggregation of these terms see: Tannya D. Jajal, "Distinguishing between Narrow AI, General AI and Super AI," *Medium*, May 21, 2018, https://medium.com/@tjajal/distinguishing-between-narrow-ai-general-ai-and-super-ai-a4bc44172e22. There is no single accepted definition for narrow AI. On this, see: Jess Whittlestone, Rune Nyrup, Anna Alexandrova, Kanta Dihal, Stephen Cave, and Leverhulme Centre for the Future of Intelligence, *Ethical and Societal Implications of Algorithms, Data, and Artificial Intelligence: A Roadmap for Research* (London: Nuffield Foundation, 2019) https://www.nuffieldfoundation.org/sites/default/files/files/Ethical-and-Societal-Implications-of-Data-and-AI-report-Nuffield-Foundat.pdf. Here, the term is not intended to be used with the precision needed by AI research communities or ethicists. It is, rather, intended to capture the term's general use in global discourse.

[4] For updated information on cyber operations by country, see the Council on Foreign Relations "Cyber Operations Tracker", at: https://www.cfr.org/cyber-operations/.

[5] The United States has a declared 1,373 strategic nuclear warheads deployed on 655 ICBMs. Credible estimates add roughly 6,000 additional stockpiled and retired warheads. See: SIPRI Yearbook 2020.

Strategic Nuclear Deterrence and Technology

Since 1954,[6] the United States has designed its nuclear strategy to deter the use of nuclear weapons on itself and its treaty allies and, since 1967[7], also to deter conventional attacks. This dual purpose has been retained over subsequent decades, instantiated most recently in the 2018 Nuclear Posture Review:

> *The highest U.S. nuclear policy and strategy priority is to deter potential adversaries from nuclear attack of any scale. However, deterring nuclear attack is not the sole purpose of nuclear weapons. Given the diverse threats and profound uncertainties of the current and future threat environment, U.S. nuclear forces play the following critical roles in U.S. national security strategy. They contribute to the:*
>
> - *Deterrence of nuclear and non-nuclear attack;*
> - *Assurance of allies and partners;*
> - *Achievement of U.S. objectives if deterrence fails; and*
> - *Capacity to hedge against an uncertain future.*[8]

All strategies of deterrence attempt to cause an outcome indirectly, by using physical means to generate a psychological effect. In the case of nuclear deterrence, the outcome is adversary inaction; the physical means are the quantities and effectiveness of nuclear weapons and of the systems that deliver them; and the psychological effect is the adversary's calculation that the value of inaction is greater than the value of action.

Decades of mathematizing the damage that would be caused by the use of different combinations of weapons and systems have produced a variety of force posture configurations designed, first, to reduce the likelihood that conventional conflict will escalate to nuclear conflict and second, to win a nuclear war if escalation control were to fail. Theorists and policymakers alike have long questioned the plausibility of both notions and, happily, neither has yet been tested.[9]

The conceptual foundations of strategic deterrence by comparison have been able to withstand abstract tests of logic and concrete tests of time. In addition to proving its durability, however, these tests also have reinforced the fact that strategic deterrence in practice is fragile because it relies wholly upon a mutual belief that launching a nuclear strike guarantees also receiving one. A no-nuclear launch

---

[6] "The Strategy of Massive Retaliation," Speech of Secretary of State John Foster Dulles before the Council on Foreign Relations, January 12, 1954. Accessed at: http://msthorarinson.weebly.com/uploads/4/1/4/5/41452777/dulles_address.pdf.

[7] "Final Decision on MC 14/3: A Report by the Military Committee to the Defence Planning Committee on Overall Strategic Concept for the Defense of the North Atlantic Treaty Organization Area," North Atlantic Military Committee, December 12, 1967.

[8] "Nuclear Posture Review," United States of America Department of Defense, February 2018.

[9] See for example: Sidney D. Drell and Frank von Hippel, "Limited Nuclear War," *Scientific American* 235, no. 5 (November 1976); Francis J. Gavin, "The Myth of Flexible Response: United States Strategy in Europe during the 1960s," *The International History Review* 23, no. 4 (2001), 847-875; William Burr, "Looking Back: The Limits of Limited Nuclear War," *Arms Control Today*, August 29, 2008; Jessica T. Mathews, "The New Nuclear Threat," *The New York Review*, August 20, 2020.

equilibrium is maintained, that is, even under the duress of immediate conflicts of interest when nuclear armed adversaries believe each other to have second-strike capability.[10]

Generating this belief in guaranteed retaliation has, to date, depended upon the ability of states to defend or to obscure the location of a subset of their nuclear arsenals. Defending strategic nuclear assets has taken the form of hardened missile silos, rapid launch, and dispersal, while obscuring them has been achieved through mobility and by merit of the ocean's physical properties.[11] Technologies that degrade, limit, or eliminate a state's ability to react with or to hide its nuclear arsenal thus undermine secure second-strike and upset the balance of confidence in assured retaliation. Cyber tools enabled by AI that can disrupt NC3 and the integration of sensing technologies capable of refined detection, AI software that conducts rapid and sophisticated data analysis, AI programming that can prompt devices into action, and unhumanned vehicles capable of traversing inhospitable territories for long durations thus can have significant implications for nuclear strategy.

The United States, Russia, China, Iran, and North Korea all are known to be actively pursuing these capabilities. Even if the primary intent is conventional use, there is nothing that precludes application in nuclear operations or that automatically ameliorates the implications of these technologies for strategic deterrence. Advances in dual-use military technologies are not going to slow, and no alternative to secure second-strike as the lodestone for nuclear stability has yet emerged. US nuclear strategy and that of competitors will shift to accommodate these realities in ways that reflect their current capabilities and comparative advantages and that contribute to achieving their core defense and national security objectives.

Hypersonic Missiles

Hypersonic weapons travel at lower trajectories than ballistic missiles and have the maneuverability of cruise missiles while travelling at faster speeds. They can be armed with conventional or with nuclear munitions, and many are dual-use.

Although Russia insists that its interest in hypersonic weapons is their ability to overcome missile defenses, effective, cheaper, less technologically demanding, and more proven countermeasures have long been available.[12] The potential effects of hypersonic weapons on missile defense thus are likely more a secondary benefit than a core rationale - instead, Russia's gain from hypersonic capabilities is returned in bolstering its international ego and quest for status, and compensating for an inability to

[10] Richard K. Betts, *Nuclear Blackmail and Nuclear Balance*, (Washington DC: Brookings Institution, 1987).

[11] The United States has pursued but never successfully developed or deployed strategic ballistic missile defense. It has achieved limited and demonstrated system capabilities in defending against a small number of missiles under prescribed circumstances and has had demonstrable success with theater-based missile defense. For a current accounting of US missile defense programs see: "Current U.S. Missile Defense Programs at a Glance," *Arms Control Association*: https://www.armscontrol.org/factsheets/usmissiledefense.

[12] Mark Episkopos, "Russia Wants You To Know It's Developing a New Hypersonic Missile," *The National Interest*, August 3, 2021: https://nationalinterest.org/blog/buzz/russia-wants-you-know-its-developing-new-hypersonic-missile-191163; Seth Cropsey, "Hypersonic weapons could tilt war in favor of Russia, China," *The Hills,* August 5, 2021: https://thehill.com/opinion/national-security/566534-hypersonic-weapons-could-tilt-war-in-favor-of-russia-china; "Countermeasures: A Technical Evaluation of the Operational Effectiveness of the Planned US National Missile Defense System," Union of Concerned Scientists, April 2000: https://www.ucsusa.org/sites/default/files/2019-09/countermeasures.pdf.

engage in regional quantitative balancing with the United States and NATO.[13] China, Iran, and North Korea have their own status—and regionally-motivated reasons for developing or seeking to purchase hypersonic weapons, including for use in regional contingencies.[14]

US concern about hypersonic capabilities is driven by the perception that their speed and maneuverability enable them to avoid detection, to defeat missile defenses, and to achieve surprise by compressing the time from launch to time of impact, even from long range.[15] There is currently no consensus based on testing and technical analysis that hypersonic weapons do indeed have these effects.[16]

Even assuming that they do, however, adversary hypersonic missile capabilities do not threaten the deterrence effectiveness of US strategic forces any more than do conventional adversary missile capabilities. US warheads and delivery vehicles are well distributed and more numerous than adversary hypersonic missiles will be for the foreseeable future, and awareness of the vulnerability of the most easily-targeted asset, silo-based intercontinental ballistic missiles (and the rationale for maintaining them nonetheless), preceded the deployment of hypersonic capabilities by many decades.[17] Hypersonic missiles thus do not exacerbate this condition so much as reaffirm the value of quantity, dispersion, and of air- and sea-mobile nuclear platforms.

Sensors, Unhumanned Platforms, and Artificial Intelligence (AI)

Commercial applications are driving rapid increases in the sophistication, availability, and usability of technologies that make more of the world more observable more of the time.[18] Sensors and cameras are capturing data through ever more precise physical measurement and generating refined, parseable images.[19] Tools and techniques of data manipulation, management, and programming - broadly captured under the rubric of artificial intelligence - are making enormous caches of these sensed and other data available for edge and distant analysis, and for use in internets of things (i.e. systems of

[13] "Advanced Military Technology in Russia," Chatham House, September 23, 2021: https://www.chathamhouse.org/2021/09/advanced-military-technology-russia/03-putins-super-weapons.
[14] John T. Watts, Christian Trotti, and Mark J. Massa, "Hypersonic Weapons in the Indo-Pacific Region," Atlantic Council, August 2020: https://www.atlanticcouncil.org/wp-content/uploads/2020/08/Hypersonics-Weapons-Primer-Report.pdf.
[15]"Hypersonic Weapons: Background and Issues for Congress," *Congressional Research Service*, August 25, 2021: https://sgp.fas.org/crs/weapons/R45811.pdf.
[16] Cameron Tracy, "Slowing the Hypersonic Arms Race: A Rational Approach to an Emerging Missile Technology," Union of Concerned Scientists, May 2021: https://www.ucsusa.org/sites/default/files/2021-04/slowing-the-hypersonic-arms-race.pdf; David Wright and Cameron Tracy, "The Physics and Hype of Hypersonic Weapons," *Scientific American*, August 1, 2021.
[17] "Conventional Prompt Global Strike and Long-Range Ballistic Missiles: Background and Issues," Congressional Research Service (CRS), July 16, 2021: https://sgp.fas.org/crs/nuke/R41464.pdf; Steve Fetter and Kingston Reif, "A Cheaper Nuclear Sponge," *War on the Rocks*, October 18, 2019: https://warontherocks.com/2019/10/a-cheaper-nuclear-sponge/.
[18] Nick Powers, "Advances in Sensor Technology Help Make the World if IoT See You," Arrow Research: https://www.arrow.com/en/research-and-events/articles/advances-in-sensor-technology-help-make-the-world-of-iot-see-you; "Military Sensors Market Size, Share & COVID-19 Impact Analysis, By Platform, By Component, By Application, and Regional Forecast, 2020-2027," *Fortune - Business Insights*, January 2021: https://www.fortunebusinessinsights.com/military-sensors-market-104666.
[19] For a sample of modern sensing technologies see: https://www.sciencedirect.com/topics/biochemistry-genetics-and-molecular-biology/sensor-technology.

devices that AI enables to act independently of human intervention.)[20] Energy sources are becoming more compact and longer-lived, and all of these technologies are now deployable on unhumanned platforms that operate underwater, on water, in the air, and in space.[21]

Applications of these technologies for purposes of ISR will increasingly allow all states to better identify, monitor, track, and target nuclear assets both intentionally and as a byproduct of deployments designed to acquire information for other purposes. Movement in this direction is ongoing and inevitable, and poses a direct challenge to secure second-strike. Terrestrial hiding will be increasingly difficult to achieve, and the oceans, too, eventually will become more rather than less scrutable.[22]

China and the United States are actively pursuing and putting these technologies into service. The United States has been explicit about the direct line between large ISR investments and its effort to achieve "information superiority" and "decision dominance," while China's "informationized warfare strategy" is visible in its island building in the South China Sea, its installations on Hainan, and investment in its military ISR satellite fleet.[23] Russia's ambitions for ISR at the moment exceed its capabilities, but this could change as it continues to prioritize development.[24]

In the near- and medium-term, progress toward more intrusive and more effective ISR will incentivize states with small stocks of nuclear assets to seek insurance through proliferation in number and location; it also increases the value of submarine-based deterrent forces as a means of concealing more

---

[20] This includes deep learning/machine learning but excludes general artificial intelligence – the category used to refer to fully intellectually realized, sentient AI. For a disaggregation of these terms see: Tannya D. Jajal, "Distinguishing between Narrow AI, General AI and Super AI," *Medium*, May 21, 2018, https://medium.com/@tjajal/distinguishing-between-narrow-ai-general-ai-and-super-ai-a4bc44172e22. There is no single accepted definition for narrow AI. On this, see: Jess Whittlestone, Rune Nyrup, Anna Alexandrova, Kanta Dihal, Stephen Cave, and Leverhulme Centre for the Future of Intelligence, *Ethical and Societal Implications of Algorithms, Data, and Artificial Intelligence: A Roadmap for Research* (London: Nuffield Foundation, 2019): https://www.nuffieldfoundation.org/sites/default/files/files/Ethical-and-Societal-Implications-of-Data-and-AI-report-Nuffield-Foundat.pdf. Here, the term is not intended to be used with the precision needed by AI research communities or ethicists. It is, rather, intended to capture the term's general use in global discourse.

[21] For an overview of operational energy, see: https://www.sciencedirect.com/topics/engineering/operational-energy.

[22] "The Sea-Through Sea: If the Ocean was Transparent", *The Economist*, June 7, 2016: https://worldif.economist.com/article/12151/see-through-sea

[23] Terrence J. O'Shaughnessy, "Decision Superiority Through Joint All-Domain Command and Control," *Joint Force Quarterly,* 99, November 19, 2020: https://www.16af.af.mil/News/Article/2421718/decision-superiority-through-joint-all-domain-command-and-control/; Sydney J. Freedberg Jr., "Army's New Aim is 'Decision Dominance,'" *BreakingDefense*, March 17, 2021: https://breakingdefense.com/2021/03/armys-new-aim-is-decision-dominance/; Dahm, J. Michael, *South China Sea Military Capability Series: A Survey of Technologies and Capabilities on China's Military Outposts in the South China Sea*, Johns Hopkins Applied Physics Laboratory, 2020: https://www.jhuapl.edu/Content/documents/IntroductiontoSCSMILCAPStudies.pdf; Felix K. Chang, "China's Maritime Intelligence, Surveillance, and Reconnaissance Capability in the South China Sea," *Foreign Policy Research Institute*, May 5, 2021: https://www.fpri.org/article/2021/05/chinas-maritime-intelligence-surveillance-and-reconnaissance-capability-in-the-south-china-sea/; "Challenges to Security in Space", Defense Intelligence Agency, 2019: https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Space_Threat_V14_020119_sm.pdf.

[24] "What Will Russian Military Capabilities Look Like in the Future?" RAND Research Brief, 2019: https://www.rand.org/content/dam/rand/pubs/research_briefs/RB10000/RB10038/RAND_RB10038.pdf; Dave Majumdar, "Russia Just Revealed How It Will Fight the Wars of the Future (And Its Shocking)," *National Interest*, March 27, 2018: https://nationalinterest.org/blog/the-buzz/russia-just-revealed-how-it-will-fight-the-wars-the-future-25106.

for longer. Indeed, China is undertaking both measures.[25] Russia and the United States do not yet need to expand their fleets of nuclear-powered ballistic missile submarines (SSBNs), though pressure to do so will mount as the ability to locate and to track them improves.

AI and Cyberspace

Advances in AI also create strategic risks in the highly volatile domain of cyberspace, the least-theorized and most uncontrolled medium of interstate interaction today.[26] Cyberspace, systems of digital connectivity that move data between and among electronic devices, is decentralized and geographically ubiquitous. It can be accessed by anyone at any time and is bidirectional, with actors able both to receive data into their own systems and devices and to push data into those of others. These features mean that AI - digital code or software that instructs devices to behave in particular ways - can effect a multitude of adversarial cyber actions, including espionage, crime, the dissemination and propagation of misinformation, and disruptions of function. As AI capabilities advance, so too will the sophistication and effectiveness of such efforts.

NC3 systems, composed of technologies that sense, process, analyze, visualize, and distribute information, that enable communication, or that power these functions, are not immune from cyber attacks.[27] In addition to creating risks of nuclear accidents and unintended launches, the possibility of adversarial intrusions into NC3 - by state or non-state actors – could make it possible to disable launch capabilities or to redirect targeting. If an actor were to believe it had, indeed, achieved a disabling or diverting cyber attack on an adversary's NC3, nuclear deterrence would dissolve.

All nuclear states, nuclear aspirants, and current and future non-nuclear competitors thus have incentive to invest in the tools of cyber intrusion and to seek to develop code that can cause catastrophic failures in NC3. Indeed, the cost-effectiveness of cyber tools and their applicability and threat to all societal systems - finance, commerce, communication, transportation, information, security and defense - make them especially appealing to actors who are otherwise at material disadvantage. This appeal is very well reflected in the cyber activities of both Iran and North Korea, which should not be expected to abate.[28]

China and Russia, too, have considerable offensive cyber capabilities that they will continue to develop. This is visible in China's long and growing record of aggressive cyber surveillance, espionage, and theft, and in Russia's successful deployment of cyber tools to interrupt the operation of critical infrastructure,

---

[25] "Military and Security Developments Involving the Peoples' Republic of China - 2020", Office of the Secretary of Defense, Annual Report to Congress: https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.PDF; Hans Kristensen, "Is China Planning to Build More Missile Submarines?" Federation of American Scientists, April 23, 2015: https://fas.org/blogs/security/2015/04/china-subs/.

[26] Joseph S. Nye Jr., "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 (Winter 2016/17), 44-71.

[27] "Task Force Report: Resilient Military Systems and the Advanced Cyber Threats," Defense Science Board, U.S. Department of Defense, 2013: https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-081.pdfl; M. V. Ramana and Mariia Kurando, "Cyberattacks on Russia - the Nation with the Most Nuclear Weapons - Pose a Global Threat," *Bulletin of the Atomic Scientists* 75, iss. 1, (2019).

[28] Luke McNamara "North Korea, Iran, and the Challenges of Dealing with Cyber-Capable Nuclear States," *Lawfare*, May 18, 2017: https://www.lawfareblog.com/north-korea-iran-and-challenges-dealing-cyber-capable-nuclear-states; Morten Soendergaard Larsen "While North Korean Missiles Sit in Storage, Their Hackers Go Rampant," *Foreign Policy*, March 15, 2021: https://foreignpolicy.com/2021/03/15/north-korea-missiles-cyberattack-hacker-armies-crime/.

to compromise government networks, and to conduct effective information operations.[29] The United States, too, has acknowledged that it possesses and is progressing offensive cyber capabilities.[30]

Open sources do not make available information about whether, and to what extent, these states or any other actors have targeted an NC3 system. Neither is there information readily available about the state of NC3 defenses, for good reason - though the United States has made public its intention generally to enhance them.[31]

Cyberspace will be exploited more, not less, in the future, and US nuclear strategy must address the resultant vulnerability of secure second-strike upon which the deterrence effectiveness of US strategic forces depends. Events in cyberspace are less foreseeable and their effects less predictable than those in the physical domains, both because cyberspace is accessible to state as well as non-state actors, and because machine learning and other AI techniques often create outcomes that humans neither intend nor understand. These characteristics should encourage consideration of a wide range of approaches to maximizing the defense, resiliency, and redundancy of NC3, including the pursuit of international agreements that prohibit cyber attacks on all components of the nuclear enterprise.[32]

Maintaining the Deterrence Effectiveness of US Strategic Forces

Advances in the sophistication of AI-enabled cyber operations and in systems that integrate AI with unhumanned platforms pose near- and medium-term threats, respectively, to the deterrence effectiveness of US strategic forces. Cyber defenses will never be impenetrable, and the utility of internets of things that have military applications, either directly or with adaptation, are being rapidly and continuously proved out in commercial markets.

The United States cannot prevent these trends from accelerating, and so in addition to continued investment in cyber tools and defenses, and in its own ISR capabilities, it will need to pursue international agreements. The challenges and risks of arriving at, much less implementing, arms control arrangements are well-known and non-trivial. Nonetheless, the severity of the possible consequences of NC3 intrusion means that all nuclear states have incentive to seek to constrain and, potentially, to prohibit some state behaviors and to establish mutual approaches to crisis management, prevention, investigation, and remediation of harmful activities perpetrated by non-state actors. Similarly, nuclear stability and the effectiveness of nuclear deterrence will continue to degrade unless or until states

---

[29] "China Cyber Threat Overview and Advisories," United States Cybersecurity & Infrastructure Security Agency: https://us-cert.cisa.gov/china; Josephine Wolff "Understanding Russia's Cyber Strategy," July 6, 2021: https://www.fpri.org/article/2021/07/understanding-russias-cyber-strategy/ ; Sarah Vogler and Michael Connell, "Russia's Approach to Cyber Warfare," CNA Occasional Paper, March 24, 2017: https://www.cna.org/cna_files/pdf/DOP-2016-U-014231-1Rev.pdf.

[30] "Nuclear Command, Control, and Communications (NC3) Modernization," Congressional Research Service, December 8, 2020: https://sgp.fas.org/crs/nuke/IF11697.pdf; Jim Garamone "Esper Describes DoD's Increased Cyber Offensive Strategy," *US Department of Defense News*, September 20, 2019: https://www.defense.gov/News/News-Stories/Article/Article/1966758/esper-describes-dods-increased-cyber-offensive-strategy/.

[31] Theresa Hitchens "NC3 Next Will Improve Nuke Cyber Defenses, Says STRATCOM," *Breaking Defense*, January 5, 2021: https://breakingdefense.com/2021/01/nc3-next-will-improve-nuke-cyber-defenses-says-stratcom/.

[32] Geoffrey Forden "The New Synergy Between Arms Control and Nuclear Command and Control," *Arms Control Today*, January/February 2020: https://www.armscontrol.org/act/2020-01/features/new-synergy-between-arms-control-nuclear-command-control.

implement meaningful mutual controls on the manner of use of ISR and/or the targeting of weapons systems - whether nuclear or conventional, human operated or autonomous.

While those efforts are underway, the United States can reinforce the deterrent effectiveness of its strategic forces by bolstering its mobile air- and sea-based nuclear capabilities. The ocean will remain the environment that is least penetrable to ISR for the longest period of time. Investments in land-based ICBMs by contrast, and especially those in silos, can be argued to be useful to deterrence generally, but are not meaningful responses to emerging technologies. Even if hypersonic missiles achieve their most optimistically predicted effects in speed and maneuverability, because US second-strike is insured by its air and ocean assets, these characteristics do not add vulnerability to general nuclear deterrence. The equation works in the opposite direction, too – US retaliatory capabilities are sufficient without the introduction of hypersonic vehicles.

How the United States and its competitors manage their integration of emergent technologies for purposes of ISR, and the extent to which they independently and multilaterally seek to protect NC3 systems from state- and non-state compromise, will define the global risk of nuclear war for the foreseeable future. Keeping that risk low will require the United States to be intentional in the manner in which it pursues emerging technologies and be measured in its reactions to the efforts of others to do the same.