Chapter 2
Nuclear Deterrence and Arms Control: From the Perspective of Developments in New Combat Domains and Emerging Technologies

ARIE Koichi

Introduction

Today, the traditional combat domains of land, sea, and air are becoming increasingly strongly linked to newer combat domains such as space, cyberspace and the electromagnetic spectrum, and cognition. During Russia's invasion of Ukraine from February 2022, Ukraine's satellite communications have been subjected to cyber and electromagnetic attacks, disrupting Internet services and other telecommunications services.[1] Additionally, while not part of a military operation, it was reported that China engaged in large-scale cognitive warfare employing deep fakes, disinformation, and other means, to interfere with Taiwan's presidential election in January 2024.[2]

The impact of activities such as these in new combat domains is also beginning to impact the nuclear domain. In February 2024, there were reports concerning suspicions that Russia was developing a new nuclear weapon to use in attacks on space satellites.[3] While the space domain has been strongly linked to the nuclear domain since the days of the Cold War, technological advancements in recent years appear to be strengthening this linkage. Developments in the cyber domain are also now impacting the nuclear domain, as exemplified by the case of Stuxnet, which was uncovered in 2010. The Stuxnet malware was used to infiltrate centrifuge control systems at a uranium enrichment facility in Natanz, Iran, causing physical damage to over 1,000 centrifuges. The malware is believed to have been deployed, via a USB drive, to computers that were not connected

---

1 Juliana Suess, "Jamming and Cyber Attacks: How Space is Being Targeted in Ukraine," RUSI, April 5, 2022; James Pearson, "Russia Downed Satellite Internet in Ukraine – Western Officials," *Reuters*, May 11, 2022.

2 Helen Davidson, "Cognitive Warfare and Weather Ballons: China Accused of Using 'All Means' to Influence Taiwan Vote," *Guardian*, January 9, 2024.

3 Johnny Franks, "Russia to Deploy Space-Based, Nuclear Anti-Satellite Weapon," *Warrior Maven*, February 18, 2024.

to the Internet.[4] In the electromagnetic domain as well, it has been suggested that directed-energy weapons could be used in the near future to disable the guidance and communications systems of theater-level nuclear weapons, rendering them ineffective.[5]

Advancements in emerging technologies such as artificial intelligence (AI), hypersonic weapons, and quantum technologies should also not be overlooked when considering the impact of developments in new combat domains. It has been pointed out that AI may be employed in space warfare in the future.[6] Emerging technologies can in this way act as enablers of conflict in new domains and they are expected to significantly influence developments in these areas. It is also expected that AI will come to be used in the cyber domain, and it is said that the use of advanced AI-based cyberattacks to hack nuclear-missile-armed strategic nuclear submarines (SSBNs) cannot be ruled out.[7]

In light of the fact that developments in these new combat domains and emerging technologies are now also having an impact on the nuclear domain, in this paper I would like to examine whether these developments will have a stabilizing or destabilizing effect on nuclear deterrence. Based on this, I will examine policy issues relating to the re-stabilization of nuclear deterrence should developments in new combat domains and emerging technologies lead to its destabilization, and conclude with additional remarks on arms control covering these domains and technologies.

Do Developments in New Combat Domains and Emerging Technologies Stabilize Nuclear Deterrence?

Of the systems used by nuclear powers to control their nuclear arsenals, it is NC3 (nuclear command, control, and communications) systems that are used for core functions such as early warning, command activity, and telecommunications, and many of the functions of these NC3 systems are dependent on satellites.[8] These satellites are vulnerable to physical attacks and electromagnetic or laser interference, and can also easily become the target of

---

4 Bishr Tabbaa, "Zer0 Days: How Stuxnet Disrupted the Iran Nuclear Program and Transformed Computer Security," *Medium*, July 17, 2020.

5 Justin Anderson and James R. McCue, "Deterring, Countering, and Defeating Conventional-Nuclear Integration," *Strategic Studies Quarterly*, Spring 2021, p. 48.

6 Charles Beames, "AI in Space and Its Future Use in Warfare," *Forbes*, December 21, 2022.

7 James Johnson, "The AI-Cyber Nexus: Implications for Military Escalation, Deterrence and Strategic Stability," *Journal of Cyber Policy*, vol. 4, no. 3, 2019, p. 448.

8 Marie Villarreal Dean, "U.S. Space-Based Nuclear Command and Control: A Guide," Center for Strategic and International Studies, January 13, 2023, pp. 1-5.

cyberattacks. The various computer systems and telecommunications networks that form an NC3 system are themselves also vulnerable to attacks in new combat domains such as the cyber and electromagnetic domains.

To date, however, no significant attacks have been made on the NC3 systems of nuclear powers. One reason for this is perhaps the understanding among the countries concerned that any preemptive strike on an NC3 system in the space, cyber, or other new combat domain would inevitably provoke a severe retaliation. It has been posited, for instance, that, as both the United States and China have expanded their military capabilities in the space and cyber domains, they are becoming mutually vulnerable to attacks in these domains, and this may encourage both to refrain from carrying out such attacks.[9] In other words, the establishment of a certain level of mutual vulnerability in these new combat domains may encourage greater caution among the countries concerned and thereby contribute to increased crisis stability.[10]

The surprising level of difficulty involved in executing attacks in the new combat domains could also deter potential attackers. In the space domain, for example, one might deploy a satellite equipped with an electromagnetic wave generator on the same orbit as a target satellite and move it close enough to conduct an attack. In addition to the significant technical costs and limitations involved in an electromagnetic attack of this nature, however, it is also highly likely that any such unusually close-range maneuvers by an attacking satellite would be detected through SSA (space situational awareness) activities,[11] meaning the preparation and execution of the attack would entail a considerable degree of difficulty. With regard to cyberattacks against satellites, it would be difficult to accurately assess their effectiveness, and similarly to what has been seen with cyberattacks like Stuxnet in 2010 and NotPetya in 2017, there is a risk that malware could infect not only the target satellite but networks worldwide as well, including the networks of the attacking side.[12]

Integrating emerging technologies into NC3 systems could enhance ISR

---

9 David C. Gompert and Phillip C. Saunders, *The Paradox of Power: Sino-American Strategic Restraint in an Age of Vulnerability* (Washington, D.C.: National Defense University Press, 2011), pp. 2-7.

10 Jacek Durkalec, Paige Gasser, and Oleksandr Shykov, "Multi-Domain Strategic Competition: Rewards and Risks," Workshop Summary, Center for Global Security Research, Lawrence Livermore National Laboratory, November 2018, p. 12.

11 Sitki Egeli, "Space-to-Space Warfare and Proximity Operations: The Impact on Nuclear Command, Control, and Communications and Strategic Stability," *Journal for Peace and Nuclear Disarmament*, vol. 4, no. 1, 2021, pp. 124-125.

12 James Timbie and James O. Ellis Jr., "Technology, Complexity, Uncertainty, and Deterrence," Kissinger Center Papers, May 2023, p. 18.

(intelligence, surveillance, and reconnaissance) capabilities targeting the nuclear weapon systems of adversaries, enhance the analysis of collected data, and also enable more appropriate decision-making concerning the use of nuclear weapons. If integrating AI into NC3 early warning systems could, for example, allow for a precise understanding of an adversary's nuclear posture, it would make it more difficult for the adversary to secretly prepare a nuclear strike. Since this would make it possible to correctly discern whether an adversary's nuclear threats were genuine, it would increase the reliability of deterrence and reduce the risk of accidental escalations during crises.[13] If high-sensitivity sensors based on quantum technologies could be used to measure variations in magnetic or gravity fields caused by SSBNs cruising underwater, it would likely become easier to detect and track them.[14] If quantum sensors can be used to detect the movements of an adversary's SSBNs, it would make calmer responses to nuclear threats possible and contribute to more appropriate decision-making concerning the use of nuclear weapons.

Do Developments in New Combat Domains and Emerging Technologies Destabilize Nuclear Deterrence?

Attacks in the new combat domains could conversely undermine the second-strike capabilities of nuclear powers, thereby destabilizing nuclear deterrence. As discussed above, NC3 systems are vulnerable to attacks in the new domains. If the various satellites that constitute these systems are destroyed or incapacitated, a nuclear power might lose the ability to execute a retaliatory nuclear strike. Cyberattacks that disrupt NC3 early warning systems, cut off communications so that nuclear attack orders cannot be received, or destroy the software of nuclear delivery systems rendering them unable to launch, could also weaken a nuclear power's second-strike retaliatory capabilities.[15]

The employment of emerging technologies could also lead to the destabilization of nuclear deterrence. It is conceivable that emerging technologies such as AI, hypersonic weapons, and quantum technology could be used to enhance the abilities of countries to detect, track, and precisely strike and destroy nuclear weapons, thereby weakening the second-strike retaliatory capabilities of adversaries and destabilizing nuclear deterrence.

---

[13] Edward Geist and Andrew J. Lohn, "How Might Artificial Intelligence Affect the Risk of Nuclear War?" RAND Corporation, 2018, p. 21.

[14] Katarzyna Kubiak, "Quantum Technology and Submarine Near-Invulnerability," European Leadership Network, December 2020, pp. 3-9.

[15] Eva Nour Repussard, "Cyber-Nuclear Nexus: How Uncertainty Threatens Deterrence," Project on Nuclear Issues, CSIS, May 10, 2023.

According to one study, if the adoption of new technologies like AI, cloud computing, and data analytics makes it easier to detect and track the second-strike capabilities of nuclear powers, particularly mobile ground-launched nuclear missiles, nuclear deterrence could be destabilized. A specific concern is that, if a nuclear power moves or disperses its nuclear missiles to avoid detection and tracking by an adversary using an ISR system enhanced with AI and other technologies, the adversary might misinterpret these actions as a signal that the state is prepared to escalate to nuclear war, increasing their motivation to conduct a first-strike attack. There is also a risk that nuclear powers, fearing the weakening of their second-strike retaliatory capabilities due to the employment of AI, may seek to bolster their nuclear forces, triggering a nuclear arms race.[16]

Attacks in new combat domains could also potentially trigger unintended escalations or cause misinterpretations by the attacked party, developing into situations where nuclear weapons could be used. The United States, China, and Russia in particular are all enhancing counterspace and cyberattack capabilities that could be used to target each other's NC3 systems. All three nations understand that a surprise attack on their own NC3 systems using such capabilities would undermine strategic stability. During an international crisis, the military forces of these countries would likely intensify their monitoring activities to avoid missing any signs of impending attacks on their nuclear weapons systems. Under these circumstances, if a localized non-nuclear (conventional) conflict involving the United States, China, and Russia were to break out, it is conceivable that they might attempt to enhance the effectiveness of their own non-nuclear operations by employing counterspace or cyberattack methods to target the command and control systems supporting their adversary's conventional operations. In many cases, however, the command and control systems for conventional operations in these countries are also used to support their NC3 systems.[17] Thus, even if the intent is to avoid targeting an adversary's NC3 system and focus solely on non-nuclear command and control systems, the result could be an inadvertent attack on an NC3 system, increasing the risk of escalation to nuclear warfare.

There are concerns that, should emerging technologies be incorporated into nuclear weapons systems, the risk of unintended nuclear weapon use could increase due to

---

16 Paul Bracken, "The Hunt for Mobile Missiles: Nuclear Weapons, AI, and the New Arms Race," Foreign Policy Research Institute, September 21, 2020.

17 Benjamin Bahney and Anna Peézeli, "The Role of Nuclear-Conventional Intermingling on State Decision-Making and the Risk of Inadvertent Escalation," NSI, November 2021, pp. 7-8.

misunderstandings, misperceptions, miscalculations, accidents, and so on.[18] In particular, the incorporation of AI into NC3 systems is seen as a particularly serious destabilizing factor for nuclear deterrence. AI is likely to be incorporated into four areas of NC3: communications, early warning systems, decision-making support, and automation of retaliatory strikes.[19] Of these, the use of AI in decision-making support and the automation of retaliatory strikes is particularly controversial. There are concerns that the decision-making algorithms of AI systems could lead to unintended actions, thereby increasing the risk of escalation into an accidental nuclear war.[20] An example of automation of retaliatory strikes is Russia's automated nuclear retaliation system, reportedly established during the Soviet era. The system is designed to respond automatically in the event that Russia's leadership is wiped out by a nuclear attack. It has been pointed out, however, that the system's sensors could misinterpret natural phenomena, such as a meteor strike, as a nuclear attack, potentially leading to unintended use of nuclear weapons.[21]

Policy Issues Relating to Re-Stabilization of Nuclear Deterrence

Given the potential destabilizing effects of developments in new combat domains and emerging technologies on nuclear deterrence, I would like to examine the policy issues relating to its re-stabilization. Let's first examine the stabilization of direct deterrence. First of all, work is required to foster shared understanding among the countries concerned regarding deterrence in new combat domains. It will be particularly crucial to work on developing an unspoken mutual understanding among countries about the activities in these new domains that can be tolerated and those that cannot. Until tacit mutual understanding on this is established to a sufficient degree, however, there is potential for some countries to attempt to justify extremely destructive attacks in the cyber domain, for example. There tends to be ambiguity and lack of clarity in the understanding among the countries concerned about the types of cyberattacks that are considered tolerable, and this could lead to unintended, accidental escalations. Prolonged competition in

---

[18] Tosaki Hirofumi, "*Shinko Gijutsu to Kaku Yokushi Kankei*" (Emerging Technologies and Nuclear Deterrence Relationship), Japan Institute of International Affairs, March 30, 2021.

[19] Jill Hruby and M. Nina Miller, "Assessing and Managing the Benefits and Risks of Artificial Intelligence in Nuclear-Weapon Systems," NTI, August 2021, pp. 12-25.

[20] Amber Afreen Abid, "Artificial Intelligence in the Nuclear Age," Strategic Vision Institute, October 4, 2023.

[21] Anthony M. Barrett, "False Alarms, True Dangers? Current and Future Risks of Inadvertent U.S.-Russian Nuclear War," RAND Corporation, 2016, p. 11.

new combat domains between concerned countries could lead to relative power shifts, destabilizing the balance of power and potentially also resulting in armed conflict.[22] It would therefore be wise to establish a common framework to share with potential adversaries to help assess the types of attacks in new combat domains that could be considered proportional and the types that are more likely to provoke escalation.[23]

A second critical policy issue is the establishment of a system able to continuously monitor emerging threats in new combat domains and detect threats to NC3 systems at an early stage. The U.S. military has already established surveillance systems for the space and cyber domains, and conducts monitoring in the cyber domain and SSA activities on an ongoing basis. Not all threats to NC3 systems can be detected, however. While SSA capabilities relating to the monitoring of space debris and other objects to prevent collisions with satellites have improved, and the ability to detect physical attacks on satellites is presumably possible to some extent, detecting non-physical attacks could be difficult. Although the forensics techniques used in investigating cyberattacks have advanced, cyberattack techniques are also constantly evolving, which limits the effectiveness of forensic capabilities in the cyber domain.[24] Overcoming these challenges is likely to incur substantial costs, but investing in the early detection of a wide range of threats to NC3 systems in new combat domains, as well as in measures to prevent the destabilization of nuclear deterrence, should be regarded as essential.

Thirdly, measures must be taken to enhance the resilience of NC3 systems in order to counter the destabilization of nuclear deterrence. Strengthening the resilience of satellites and other space assets, is a particularly urgent issue, and it is also crucial for establishing a deterrence-by-denial posture. Specific measures include deploying decoy satellites and defensive escort assets in orbit and increasing the number of satellites.[25]

Next, with regard to the stabilization of extended deterrence, I will focus on countries under the U.S. nuclear umbrella that rely on the United States for extended nuclear deterrence. Firstly, it is necessary to consider responses to situations where attacks in new combat domains are directed not at the United States itself, but at countries

---

[22] Michael P. Fischerkeller and Richard K. Harknett, "What Is Agreed Competition in Cyberspace?" *Lawfare*, February 19, 2019.

[23] Vincent Manzo, "Deterrence and Escalation in Cross-Domain Operations: Where Do Space and Cyberspace Fit?," *Strategic Forum*, no. 272, December 2011, pp. 3-7.

[24] Suzuki Kazuto, "*Anzenhosho no Kukanteki Henyo*" [Spatial Transformation of Security], Kokusai Mondai (International Affairs), no. 658 (January/February 2017): p10.

[25] Michael P. Gleason and Peter L. Hays, "Getting the Most Deterrent Value from U.S. Space Forces," Center for Space Policy and Strategy, October 2020, pp. 4-5.

under the U.S. nuclear umbrella. Possible scenarios include cases where the space assets of an "umbrella state" are subjected to non-physical attacks such as jamming or where its command and control systems are targeted by cyberattacks.[26] To avoid the destabilization of extended deterrence in such cases, the division of roles needs to be clarified as much as possible with regard to those cases that should be deterred or responded to as an alliance, and those that the umbrella state should handle independently.

Secondly, it is also important for umbrella states and the United States to maintain a shared understanding about the potential for emerging technologies to destabilize nuclear deterrence. When AI is incorporated into the NC3 system of the United States, for example, it would be preferable that there be consultations between umbrella states and the United States to discuss and align their perspectives on issues such as the NC3 functions that AI is to be used in and whether its introduction will destabilize nuclear deterrence. It would also be necessary to discuss issues relating to nuclear deterrence in cases where AI is incorporated into systems that support non-nuclear operations where these non-nuclear systems are also linked to NC3 systems. The United States is advancing the Joint All-Domain Command and Control (JADC2) concept, which is aimed at connecting all "sensors and shooters" in the U.S. military in real-time for combat purposes.[27] In the future, the JADC2 concept may be merged into a new command and control system that supports the U.S. military's non-nuclear operations, and the possibility that AI could be introduced into this system and then eventually linked to the NC3 system cannot be denied.[28] Given that, as mentioned above, the command and control systems supporting non-nuclear operations are also used to support NC3 systems, the incorporation of AI into the JADC2 system should be understood as an action that could also impact the U.S. NC3 system. Taking this into account, umbrella states ought to deepen discussions with the United States on the direction for extended nuclear deterrence in new combat domains.

Thirdly, from the perspective of umbrella states, it may be worth considering proposing an agenda for extended nuclear deterrence in the context of new combat domains and

---

[26] Dean Cheng, "Prospects for Extended Deterrence in Space and Cyber: The Case of the PRC," Heritage Foundation, January 21, 2016.

[27] Kikuchi Shigeo, "*Chugoku no Gunjiteki Kyoi ni Kansuru Ninshiki Henka to Beigun Sakusen Konseputo no Tenkai: Togo Zen Domein Shiki Tosei* (JADC2) *o Chushin ni*" (China as the "Pacing Threat": Evolving U.S. Operational Concepts and Joint All-Domain Command and Control (JADC2)), Anzenhosho Senryaku Kenkyu (Security & Strategy) volume 2, No. 2 (March 2022).

[28] Michael Klare, "The Military Dangers of AI Are Not Hallucinations," *Foreign Policy in Focus*, July 14, 2023.

emerging technologies, and initiatives to incorporate this into their alliance's nuclear policy. NATO has, for this purpose, a framework for nuclear consultations based on the Nuclear Planning Group (NPG), in which nearly all NATO member states participate. While there are no multilateral frameworks like NATO's NPG in the Indo-Pacific region, umbrella states would likely be able to propose an agenda for extended nuclear deterrence in connection with new combat domains within the framework of their bilateral nuclear consultations with the United States.

Arms Control Relating to New Combat Domains and Emerging Technologies

In light of the potential for destabilization of nuclear deterrence due to developments in new combat domains and emerging technologies, what approach to arms control ought to be pursued? First, given that anti-satellite capabilities pose a threat to NC3 space assets, regulating such capabilities ought to be, from the perspective of preventing the destabilization of nuclear deterrence, a focal point of arms control in the space domain. China and Russia have maintained a posture of seeking an arms control treaty to regulate the deployment of weapons in space, while the United States and other Western countries consider the greatest threat to space security not to be specific weapons but *behavior and actions* in orbit, and are instead adopting an approach aimed at establishing norms for responsible behavior and actions in space.[29] This approach of the West in pursuing the establishment of a code of conduct is based on the recognition that defining what constitutes a "weapon" in space is difficult, and that a traditional arms control approach aimed at regulating and controlling specific weapons, as pursued by China and Russia, would therefore lack effectiveness and make verification practically impossible.

As is the case in the space domain, defining what constitutes a "weapon" in the cyber domain is also challenging, and a traditional arms control approach may fail to ensure effectiveness and transparency. Instead of a traditional approach aimed at banning or regulating cyberweapons, therefore, it would be more meaningful from an arms control perspective to focus on regulating specific behavior and actions that have a destabilizing effect on nuclear deterrence, such as cyberattacks targeting NC3 systems.

With regard to the electromagnetic domain as well, given the potential for directed

[29] Victoria Samson, "Breaking the Impasse over Security in Space," Arms Control Association, September 2022.

energy weapons to incapacitate theater-level and sub-theater-level nuclear weapons systems, it would be desirable to consider frameworks to restrict the use of directed energy weapons against such systems. U.S. B61-12 tactical nuclear bombs, which the United States is deploying to five other NATO member states, are equipped with inertial guidance systems to improve accuracy,[30] and if these guidance systems are vulnerable to directed energy weapons, then the abovementioned frameworks would likely also contribute to the stabilization of NATO's nuclear deterrence. Instead of a traditional approach of regulating the directed energy weapons themselves, however, it would be preferable to pursue a normative approach focused on regulating behavior and actions relating to the use of directed energy weapons that have the potential to destabilize nuclear deterrence.

Considering the risks associated with the integration of emerging technologies into NC3 systems, arms control to regulate their use is also necessary. With respect to AI in particular, as AI has not yet reached a sufficient level of technological maturity for nuclear powers to be confident in integrating it into their NC3 systems, there have been calls for nuclear powers to move quickly to reach an agreement on regulating against the use of AI in ways that could destabilize nuclear deterrence and increase the risk of nuclear weapons use.[31] Rather than a traditional arms control approach of regulating AI as a "weapon," a normative approach that seeks to prevent behavior and actions that could destabilize nuclear deterrence through the use of AI seems more meaningful. There is also a possibility that cyberattacks targeting nuclear weapons systems incorporating AI could rewrite AI training data sets and render the systems inoperative.[32] It may be necessary to consider whether such cyberattacks targeting the AI incorporated into nuclear weapon systems and other such specific actions should also be designated as behavior that ought to be prevented.

Among emerging technologies, it is hypersonic weapons that present the possibility of applying traditional approaches to weapon regulation. By proposing limitations on hypersonic weapons to Russia, the United States could advance strategic nuclear arms reduction negotiations advantageously with Russia, and reestablish upper limits on intermediate-range nuclear forces. This could open up a pathway towards a U.S.-Russia nuclear arms control agreement, and it has been pointed out that it would be desirable

---

30 "B61-12 Nuclear Bomb," *Airforce Technology*, November 6, 2020.

31 Lauren Kahn, "Mending the 'Broken Arrow': Confidence Building Measures at the AI-Nuclear Nexus," *War on the Rocks*, November 4, 2022.

32 Zachary Kallenborn, "AI Risks to Nuclear Deterrence Are Real," *War on the Rocks*, October 10, 2019.

to also eventually involve China.[33] It should be noted, however, that during such negotiations, Russia and China would both likely demand the inclusion of U.S. missile defense systems as a target for regulation in such an agreement. China and Russia's development of hypersonic weapons was originally motivated by their desire to secure second-strike retaliation capabilities in response to the superiority of U.S. missile defense capabilities. Given this context, China and Russia may both view, on balance, limitations on U.S. missile defense as a beneficial trade-off for the restriction of hypersonic weapons. If, therefore, the regulation of hypersonic weapons comes to be included in future U.S.-Russia (or U.S.-Russia-China) arms control talks, it is likely to be discussed in connection with restrictions on U.S. missile defense systems.

Conclusion

Future developments in the new combat domains and emerging technologies will likely have a significant impact on nuclear deterrence and arms control. The United States, China, and Russia are competing fiercely to develop new technologies in the context of great power competition, and by enabling conflict in new domains, these technologies contribute to the destabilization of nuclear deterrence. In this paper, I have explored the potential for a normative code of conduct-based approach as a form of arms control to mitigate the destabilization of nuclear deterrence due to developments in new combat domains and emerging technologies. It goes without saying, however, that such an approach would involve many challenges, such as finding ways to verify compliance. Amid these developments, U.S. national security advisor Jake Sullivan stated in June 2023 that the United States would resume its efforts to bring China into arms control negotiations. He also stated the United States would maintain its nuclear deterrent while supplementing its current strategic nuclear forces with new technologies like non-nuclear precision strike weapons. He also indicated, however, that from an arms control perspective, the United States would seek to establish a global agreement ensuring that AI would not be used to authorize nuclear strikes without human involvement ("maintaining a human in the loop").[34] This stance of the United States is perhaps noteworthy, as it offers a glimpse into the future trajectory of arms control in relation to emerging technologies.

---

[33] Spenser A. Warren, "Avangard and Transatlantic Security," Center for Strategic and International Studies, September 23, 2020.

[34] Julian E. Barnes and David E. Sanger, "U.S. Will Try to Bring China into Arms Control Talks," *New York Times*, June 2, 2023.