Chapter 3

New Domains and Nuclear Weapons Systems

The Implications for Nuclear Deterrence and Arms Control

ARIE Koichi

Japan Air Self-Defense Force's space operations unit conducting training (Kyodo)

In recent years, operations in "new domains," including space, cyberspace, and the electromagnetic spectrum, have been impacting warfare in the traditional land, sea, and air domains, while emerging technologies, such as artificial intelligence (AI) and quantum technology, are being integrated into operations in new domains. The impact of such operations and emerging technologies are now extending to the nuclear domain, presenting a new challenge for the nuclear weapons systems of nuclear-armed states: how can the systems deter aggression in new domains, coupled with fulfilling their original mission of deterring aggression in the land, sea, and air domains?[1]

The security literature on these topics include studies on "cross-domain deterrence" (CDD).[2] CDD is considered to be a variant of "complex deterrence," which was presented in the 2000s as a new deterrence concept to adapt to the drastically different strategic environment following the Cold War.[3] Erik Gartzke from UC San Diego and Jon Lindsay from the University of Toronto[4] define CDD as the use of threats in one domain or a combination of several different threats to prevent actions that will change the status quo in another domain.[5] However, CDD is not without challenges, including those relating to the credibility of deterrence threats and escalation control.[6]

Including CDD, various arguments have been made regarding the impact of operations in new domains on deterrence, especially nuclear deterrence. Some posit that any state would be cautious of aggression in new domains because a preemptive strike in the space or cyberspace domain would trigger major retaliation of some form, including nuclear. Others have raised concerns that operations of hostile countries in space, cyberspace, and other new domains may incentivize nuclear-armed states to carry out a preemptive strike that would destabilize nuclear deterrence.[7] Some contend that the use of emerging technologies by one nuclear-armed state could potentially destabilize its nuclear deterrence relationship with other nuclear-armed states.[8] Tosaki Hirofumi from the Japan Institute of International Affairs points out that the integration of emerging technologies into nuclear weapons systems contributes to the stabilization of the deterrence relationship between nuclear-armed states on the one hand, while facilitating the destabilization of the deterrence relationship on the other hand.[9]

Building on such discussions, this chapter first provides an overview of the link between new domains and nuclear weapons systems, and examines whether the impact of new domains on nuclear weapons systems stabilizes or destabilizes nuclear deterrence. It then considers policy challenges for enhancing deterrence stability if the effects of new domains were destabilizing nuclear deterrence. Furthermore, it attempts to explore

arms control approaches in new domains. With emerging technologies expected to impact operations in new domains, including consideration of AI technology applications in cyber and cognitive warfare, this chapter discusses new domains along with emerging technologies.

The Link between New Domains and Nuclear Weapons Systems

Space Domain

Among the new domains, space has been closely connected to nuclear weapons systems even from the Cold War era, and in this sense, is not necessarily a new domain. Within the U.S. nuclear weapons system, the nuclear command, control, and communications (NC3) system enables early warning of ballistic missiles, command and communications, and other central roles, many of which rely on satellites.[10] These satellites serve to not only perform nuclear operations but oftentimes also support non-nuclear (conventional) operations. This "entanglement" of nuclear and non-nuclear systems has increasingly become a concern in recent years,[11] a key issue that cannot be overlooked in considering the relationship between the space domain and nuclear weapons systems.

Space assets, including satellites, are vulnerable to various types of attack. Counterspace systems, which are means of attacking space assets, include kinetic physical, nonkinetic physical, electronic, and cyber capabilities. Kinetic physical directly attacks satellites and has physical effects. Specifically, weapons such as a direct-ascent anti-satellite missile launched from land or a co-orbital satellite deployed in space destroy or incapacitate the target satellite. Nonkinetic physical uses weapons such as a laser weapon or a high-power microwave (HPM) weapon to physically damage the target satellite. Electronic involves jamming or spoofing radio frequency signals used for data exchange between satellites and terrestrial stations. By contrast, cyber capabilities target and attack space asset data and the systems that use and manage the data.[12]

As of date, the United States, China, Russia, and India have successfully test-destroyed their own satellites using direct-ascent anti-satellite missiles, a kinetic physical weapon. However, no country has ever attacked another country's satellite.[13] As regards nonkinetic physical weapons, China is believed to possess ground-based laser systems capable of blinding or damaging optical sensors on low-orbit satellites, while Russia may have developed the Kalina laser system with a similar capability.[14] Russia is

reported to have already deployed the Peresvet ground-based laser system with limited offensive anti-satellite capabilities, although the details are unknown.[15]

Cyberspace Domain

Unlike space, cyberspace is a relatively new domain for nuclear weapons systems. Among the first uses of cyberspace reported is the discovery of vulnerabilities in the radio system used to transmit nuclear missile launching orders to the U.S. Navy's ship, submersible, ballistic, nuclear (SSBN) submarines in the 1990s, which nearly resulted in outside hackers taking over the Navy's radio transmitter in the state of Maine.[16]

The above example partially overlaps with electronic warfare in the electromagnetic domain. With increasing computerization, digitization, and networking of weapons systems, the cyberspace domain began to overlap with the electromagnetic domain. Specifically, computers connected to networks access the cyberspace through digital means of communication, such as wires, fiber-optic cables, microwave relays, and satellite communications—all of which are applications of electromagnetic waves.[17] As more digital information is exchanged via the cyberspace and electromagnetic domains, nuclear weapons systems have also become more susceptible to the threat of cyber attacks targeting digital information.

Hacking into nuclear weapons systems was initially considered impossible and has not occurred to date. It is possible, however, for attacks to target personnel lacking cybersecurity knowledge or to target system failures.[18] In fact, in December 2020, it was revealed that the network of the National Nuclear Security Administration that administers U.S. nuclear weapons was hacked, albeit not the nuclear weapons system itself.[19] Furthermore, from August to September 2022, three U.S. national laboratories researching nuclear-related technologies—Brookhaven, Argonne, and Lawrence Livermore—were targets of cyber attacks by Russia's Cold River. The hacking group created fake login pages for each laboratory and sent emails to nuclear scientists in an attempt to steal their passwords. The laboratories have not commented on the incidents, and it is unclear whether the cyber attacks were successful.[20]

While all of these cyber attacks targeting nuclear-related facilities were conducted over the Internet, cyber attacks not involving the Internet have also taken place. A notable example is the Stuxnet incident that became public in 2010. Stuxnet infected the control system of centrifuges at the uranium enrichment facility in Natanz, Iran. A malware that physically damaged over 1,000 centrifuges is believed to have infected a device

unconnected to the Internet via a USB stick.[21]

Electromagnetic Domain

As already revealed, nuclear weapons systems, including communications, rely heavily on the electromagnetic environment, making the systems prone to the effects of electronic warfare. In particular, electronic attacks, such as jamming and spoofing, have a major impact on system functions.[22] The jamming of communication signals between an NC3 satellite and terrestrial station, as was already mentioned, can be conducted on both the uplink communication from the terrestrial station to the satellite and the downlink communication from the satellite to the terrestrial station. While uplink jamming is considered to be technically more challenging because it requires more power to reach the satellite, jamming satellite communications in general is relatively easy to do and not very costly. Moreover, it is hard to determine whether communication disruption is due to intentional jamming or to signal disturbance or interference. The difficultness of identifying the origin of attack offers another advantage for the offender.[23]

Other aggressions using the electromagnetic spectrum include an electromagnetic pulse (EMP) attack. EMP refers to powerful electromagnetic energy released by events such as a nuclear explosion. It damages or destroys all electronic equipment and cripples critical social infrastructure, including the power grid.[24] As part of the measures for strengthening the nuclear weapons system against EMP attacks, the U.S. Air Force is considering enhancing the B-2 stealth strategic bomber's ability to withstand an EMP.[25]

The United States is developing the High-powered Joint Electromagnetic Non-Kinetic Strike Weapon (HiJENKS), an HPM weapon that can locally emit EMP without a nuclear explosion and is capable of destroying an adversary's electronic equipment. HiJENKS is being jointly developed by the U.S. Air Force and Navy, building on the achievements of the former's HPM weapon project known as the Counter-electronics High-powered Microwave Advanced Missile Project (CHAMP). Equipped with the latest technology, HiJENKS is smaller than the air-to-ground missile-mounted CHAMP and is said to be able to operate in a harsher environment.[26]

The Russian military's electronic warfare unit (Sputnik/Kyodo News Images)

The Air Force reportedly deployed at least 20 CHAMP cruise missiles with warheads in 2019.[27]

Research and development are also under way to use lasers and HPM weapons for missile defense. Notably, the United States has begun exploring the combination of laser weapons with current interceptor missiles to intercept ballistic missiles and hypersonic missiles in the future.[28] Justin Anderson from the U.S. National Defense University and James R. McCue from the U.S. Air Force indicate that directed-energy weapons may be used in the near future to make the guidance systems and communications of theater-level nuclear-capable weapons dysfunctional and fatally compromise the nuclear weapons.[29]

Cognitive Domain

Cognition is defined as a process of human thinking, encompassing acts such as acquiring information through observation, thinking, imagination, memory, judgment, problem-solving, and selective attention.[30] Cognitive warfare, or warfare over the human cognitive domain, is considered a new domain in modern warfare, and is regarded as the art of manipulating the cognition of the opponent at both the individual and collective levels to affect their decisions and actions.[31] Methods of cognitive warfare include the spread of disinformation via social media.[32] Cyber techniques too are deemed effective in this domain. When Russia interfered in the 2016 U.S. presidential election, numerous cyber attacks targeted security vulnerabilities in the election infrastructure.[33] Additionally, electromagnetic means may be utilized in warfare in the cognitive domain. The Chinese People's Liberation Army is reportedly developing weapons that emit electromagnetic energy from HPM or other sources to directly attack the human brain and disrupt normal cognitive functions. A scholar has termed these methods of attack "NeuroStrike."[34]

The connection between the cognitive domain and nuclear weapons systems can be observed from the spread of disinformation about U.S. tactical nuclear weapons in 2016. On August 18 that year, reports circulated worldwide that the United States had moved its tactical nuclear weapons stored at Turkey's Incirlik Air Base to Romania. This was later revealed to be fake news.[35] A study on the influence of social media on nuclear decision-making, with a focus on Twitter (now X), was published in 2020.[36] Additionally, research has been conducted on the extent to which disinformation can disguise the use of nuclear weapons.[37] Rebecca Hersman from the Center for Strategic and International Studies published a paper in 2020 regarding the impact of disinformation on NC3, in which she suggests

that the dissemination of disinformation may undermine public trust in the U.S. NC3.[38]

Nuclear weapons systems have been affected by not only disinformation but also misinformation. In 2017, several major media outlets reported with photos that China officially deployed the new DF-41 road-mobile intercontinental ballistic missile (ICBM). However, subsequent investigation revealed that the reports were misinformation. The photos had been those previously shared on social media, and the missile-like object in the photos could not be confirmed to be a DF-41.[39]

Impact of Emerging Technologies

There is a global competition unfolding for the development of emerging technologies, with AI, hypersonic weapons, and quantum communication arising as critical international security concerns. Emerging technologies have the potential to significantly influence developments in new domains,[40] and high expectations are placed on them for the further modernization of nuclear weapons systems.[41]

In the future, AI may be used in warfare in the space domain. AI is expected to considerably elevate the performance of on-orbit satellites and in-ground systems. Furthermore, AI's self-learning capabilities are anticipated to upgrade algorithms autonomously based on the operational environment, giving an unprecedented competitive advantage to the side using AI in space warfare.[42]

AI may also potentially impact the cyberspace domain. If AI-augmented offensive cyber capabilities are directed at nuclear weapons systems in the future, it is expected to make it nearly impossible to detect and attribute a cyber attack and identify the origin of attack within the short timeframe in which a nuclear decision is made.[43]

According to the U.S. Department of Defense's "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2022," the People's Liberation Army is considering the use of AI in warfare in the cognitive domain. In addition to creating deep fakes, disseminating propaganda, and analyzing the sentiments of Internet users, other AI uses being considered include integrating AI into the military's bot network on social media to create authentic-like content and post it on social media platforms at the optimal time.[44]

Hypersonic weapon technology is gaining attention for offering new kinetic attack capabilities in space and other domains. These weapons can fly at Mach 5 or above through the atmosphere in the hypersonic range and maneuver at high speeds. They have a military advantage in being able to

strike targets while evading interception by existing air and missile defense systems.[45] Because hypersonic weapons are developed for use at altitudes below the boundary of atmosphere and outer space (near-space), they have the characteristic of spanning both the air and space domains.[46] In recent years, attempts have seemingly been made to use hypersonic weapons beyond near-space in the space domain. In an alleged test launch of a new hypersonic weapon conducted in 2021, China is believed to have separated the vehicle from its carrier rocket in space, placed it into low-earth orbit, and then had it re-enter the atmosphere.[47] Additionally, the United States is advancing a plan to deploy a constellation of satellites equipped with sensors to detect and track hypersonic weapons in low-earth orbit.[48] As the above reveals, the development race for hypersonic weapons and their interception means are increasingly extending into the space domain.

While China and Russia are developing and deploying both nuclear and non-nuclear hypersonic weapons, the United States does not have plans to equip its hypersonic weapons with nuclear warheads. Admiral Charles Richard, commander of U.S. Strategic Command, stated that non-nuclear hypersonic weapons provide the president with new strike options to rapidly project power without crossing the nuclear threshold and strengthen the overall U.S. strategic deterrence posture.[49]

Also increasingly being discussed is the impact of using quantum technology in nuclear weapons systems. Research and development are under way on this technology that applies the principles of quantum mechanics. The use of quantum technology is expected to dramatically improve the confidentiality of communications and encryption, enhancing the capabilities of nuclear weapons systems that require the highest level of confidentiality. According to Peter Hayes from Sydney University, integrating quantum-encrypted communication technology into the NC3 systems of nuclear-armed states can create NC3 systems that are theoretically immune to eavesdropping, jamming, and hacking.[50] China is actively working on the commercial application of quantum key distribution (QKD), a form of quantum-encrypted communication technology, and launched a Micius quantum communications experimental satellite in 2016. In 2017, China successfully used Micius to encrypt and transmit images via QKD between Beijing and Vienna, Austria and conducted a video conference between the two cities.[51]

Moreover, China is focusing on quantum sensing technologies, including quantum radar. Quantum radar is currently thought to have little military utility. However, scholars have indicated that if China succeeds in the operational deployment of a high-performance quantum radar, its ability to monitor and track nuclear weapons would improve substantially, which may

have serious implications for the U.S. nuclear weapons system.[52]

The Potential for New Domains to Stabilize Nuclear Deterrence

Mutual Restraint of Space and Cyberspace Attacks

As will be discussed later, while much has been said about NC3's vulnerability to attacks in space, cyberspace, and other new domains, this vulnerability does not necessarily imply that the origin of attack will not be identified. This may incentivize states to mutually restrain from striking each other's NC3 system. Such countries are aware that some major form of retaliation would be unavoidable if a preemptive strike is conducted in new domains and the origin of attack is identified.[53] It is not hard to imagine that a preemptive strike on NC3 much less would significantly raise the probability of nuclear retaliation.

To ponder this further, the case of cyber attacks against NC3 is drawn upon. Erica Lonergan and Keren Yarhi-Milo examine whether such cyber attacks can be used as a means of signaling in nuclear deterrence (declaring the intention to deter the use of nuclear weapons and communicating it to the adversary). They suggest that, if the United States were to launch a cyber attack against Russia's NC3 for signaling, Russia might interpret signals from U.S. cyber means as an attack on its critical military systems, provoking Russia to use nuclear weapons, contrary to the intention of nuclear deterrence. Even if nuclear weapons were not used, Russia will likely take measures that lower the nuclear threshold, such as bolstering its nuclear force posture or delegating nuclear use authority, which would increase the probability of accidental nuclear escalation. In other words, Lonergan and Yarhi-Milo argue that the United States should refrain from attacks against NC3 because such aggression, even by cyber means, largely risks breaking down nuclear deterrence.[54]

The United States and China—not only the United States and Russia—may also mutually restrain each other's attacks in new domains. According to David Gompert and Phillip Saunders from the U.S. National Defense University, both the United States and China have built up their military capabilities in space and cyberspace. As a result, they are becoming mutually vulnerable to attacks in these domains and could exercise mutual restraint in waging such attacks. However, since both countries understand that military capabilities in the space and cyberspace domains enhance the performance of the opponent's units and weapons in combat, they are unlikely to totally

eliminate the option of striking these military capabilities.[55]

Taking measures so that states do not adopt these offensive options in space and cyberspace will be critical for maintaining mutual restraint of attacks.

In the case of attacks in the electromagnetic domain, anti-satellite electromagnetic attack capabilities have severe technical constraints, which may force states to exercise mutual restraint. An example is a case in which an attacking satellite or "killer satellite" is launched into the same orbit as the target satellite, approaches the satellite, and conducts an electromagnetic attack. First, the killer satellite must carry a large amount of fuel necessary for the approach maneuvers. This increases the satellite's size and weight, making it difficult to operate covertly while evading space situational awareness surveillance. If the killer satellite is made smaller and lighter while increasing its on-board fuel, there would not be space to carry the electromagnetic emission device used for attacks. Furthermore, electromagnetic attacks require a vast amount of power, and securing this power poses another challenge: attaching solar panels to the satellite would make it more easily detectable, while carrying batteries would increase the satellite's weight, and battery performance is depleted over time. Moreover, immediately shifting to approach maneuvers after orbital insertion would arouse suspicion. Consequently, the attack might take years, during which the harsh outer space environment could degrade the killer satellite's capabilities, making it difficult to complete its electromagnetic attack mission.[56] These sizeable technical costs may induce restraint from electromagnetic attacks that employ killer satellites.

If mutual restraint of attacks in new domains continues, it can perhaps be described as a continuation of the situation outlined by the "general deterrence" concept of Patrick Morgan, one of the renowned scholars of deterrence theory. Unlike "immediate deterrence" in crises, "general deterrence" refers to a relatively stable state of deterrence without crises. In other words, when the relationship between the deterring state and the deterred state is in a state of "general deterrence," an immediate attack is not expected to occur even if at least one of the states is contemplating the use of military force given the opportunity.[57] Although "general deterrence" has numerous ambiguities compared to immediate deterrence as an analytical concept, it is a suggestive concept for elucidating the mechanisms of mutual restraint of attacks in new domains from the perspective of deterrence.

The Potential for the Cognitive Domain to Deter the Use of Nuclear Weapons

As Hersman points out, if the dissemination of disinformation can influence public perception of a nuclear-armed state's NC3 system, it may conversely be possible to mobilize broad public support for one's NC3 system and signal a strong deterrence resolve to the hostile nuclear-armed state, making it more likely to deter its use of nuclear weapons.[58] For example, a state can try to gain public support by disclosing information on social media about the credibility of their NC3 system to the extent possible, using concise and easily understandable wording. As an adversary is anticipated to disseminate disinformation or misinformation about one's NC3 system, it will be important to promptly detect and swiftly correct and/or take other appropriate actions and ensure that accurate information about one's NC3 system is communicated to the people.

Guiding the thinking of a hostile nuclear-armed state's decision-makers and affecting their situational judgment and decision-making to deter their use of nuclear weapons is one form of warfare in the cognitive domain. Paul Goossen from the U.S. Air Force calls it "cognitive targeting." He examines the possibility of controlling an adversary not to use nuclear weapons and achieving war objectives in conventional warfare with a nuclear-armed state. According to Goossen, "cognitive targeting" guides the adversary's thinking in the cognitive domain, instead of employing military force directly against the adversary's entire national capability or national will. It uses military force indirectly and in a focused manner to eliminate non-desired options from the adversary's thought process. In doing so, it is considered important to present an option acceptable to both parties as a way to exit the conflict on terms favorable to both parties and direct the adversary to select this option, rather than cornering the adversary and leaving it no way to escape. Therefore, it is essential to quickly anticipate the adversary's strategy, including actions it might take, and preemptively think ahead of the adversary to outmaneuver his strategy.[59] To deter the use of nuclear weapons by "cognitive targeting," it is necessary to skillfully use military force as a way to communicate with the adversary, which requires sophisticated strategic thinking and military operational capabilities needless to say. It is also conceivable to employ social media or other platforms to decrease the adversary's incentive to use nuclear weapons.

Constraining Nuclear Weapons Use with Emerging Technologies

A body of literature suggests that integrating emerging technologies into nuclear weapons systems will enhance their intelligence, surveillance, and reconnaissance (ISR) capabilities against an adversary's nuclear weapons system as well as increase the systems' capabilities to analyze the collected information, enabling more appropriate nuclear decisions.

Edward Geist and Andrew Lohn from RAND Corporation explain that, if AI is employed in NC3's early warning system, allowing the nuclear movements of an adversary to be monitored accurately, the adversary would find it harder to secretly prepare for a nuclear attack. As a result, a state can correctly assess whether the adversary's nuclear threat is genuine (i.e., whether it is accompanied by preparations for a nuclear strike). Geist and Lohn argue that this can increase the credibility of deterrence and reduce the danger of accidental escalation in crises.[60] Jessica Cox and Heather Williams view that AI-empowered nuclear weapons systems could lead to more accurate analysis of early warning information and provide more time to determine the need for nuclear weapons use, which in turn will contribute to the stabilization of nuclear deterrence.[61]

The application of quantum technology is expected to enhance ISR capabilities against the adversary's nuclear weapons system. For example, quantum sensors can use quantum effects to measure, with higher sensitivity than conventional sensors, various physical quantities, such as magnetic field, gravity, and angular motion.[62] Leveraging these quantum sensors may facilitate detection of enemy SSBNs, which are considered to have an invulnerable second-strike capability. Specifically, quantum sensors can potentially measure changes in magnetic field and gravity caused by submerged SSBNs and aid in their detection and tracking.[63] If quantum sensors can be used to preemptively detect the movements of an adversary's SSBNs, it would enable the adversary to respond calmly to nuclear threats and contribute to more appropriate nuclear weapons decision-making.

Emerging technologies' enhancement of ISR capabilities may also facilitate future nuclear arms control verifications. Using AI technology for ISR activities and strengthening monitoring and verification of compliance with treaty obligations are thought to increase transparency of treaty implementation and contribute to confidence-building.[64]

The Risk of New Domains Destabilizing Nuclear Deterrence

Increasing Vulnerability of Second-Strike Capability

Attacks in new domains intrinsically make second-strike capability vulnerable and destabilize nuclear deterrence. Such an attack is thought to impact nuclear deterrence by targeting and incapacitating not so much nuclear weapons themselves as NC3 systems, thereby rendering nuclear retaliation impossible or difficult and making second-strike capability vulnerable. If a cyber attack, for example, disrupts the early warning system of NC3, cuts off communications so that a nuclear attack order cannot be received, or destroys the software of nuclear delivery systems and prevents nuclear launches, this will foreseeably make a nuclear-armed state's second-strike capability increasingly vulnerable.[65]

Another possible scenario is one where a cyber attack on NC3 is followed by counterforce strikes employing emerging technologies against second-strike capabilities. For example, Barry Pavel and Christian Trotti from the Atlantic Council present a scenario where China or Russia first uses cyber attacks to disable the functions of the U.S. NC3 system, then uses hypersonic weapons to eliminate ICBM launch sites, then underwater drones and advanced sensors to capture and destroy U.S. SSBNs. In this scenario, even if the United States were to use its remaining nuclear forces to launch a retaliatory attack, all of them would be intercepted and destroyed by Chinese or Russian advanced air and missile defenses, thus incapacitating the U.S. nuclear deterrent.[66] As this example shows, if there are cyber attacks on NC3 systems and they become dysfunctional, the second-strike capabilities of nuclear-armed states will likely become vulnerable to counterforce strikes.

The impact of emerging technologies is examined next. In general, emerging technologies such as AI and hypersonic weapons are believed to destabilize nuclear deterrence by increasing the ability to detect, track, precisely strike, and destroy nuclear weapons and contributing to the increasing vulnerability of second-strike capabilities. Paul Bracken from Yale University argues that the use of emerging technologies including AI will facilitate the detection and tracking of the second-strike capabilities of nuclear-armed states, particularly ground-mobile nuclear missiles, thus destabilizing nuclear deterrence. In a crisis, nuclear-armed states will attempt to move and disperse their nuclear missiles to avoid detection and tracking by an adversary's AI- or other technology-enhanced ISR system. Other nuclear-armed states could misinterpret such movements as a signal that nuclear war would not be off the table, giving an incentive for a first strike. According to Bracken, nuclear-armed states, fearing that AI would

make their second-strike capabilities vulnerable, may embark on nuclear arms buildup, thereby inducing a nuclear arms race.[67] Because Chinese and Russian second-strike capabilities are primarily ground-mobile nuclear missiles, they will be susceptible to these impacts.

Furthermore, it has been suggested that U.S. non-nuclear hypersonic weapons may increase the vulnerability of China's and Russia's second-strike capabilities. Dean Wilkening from Johns Hopkins University contends that the two countries' ground-mobile ICBMs would become vulnerable if U.S. hypersonic weapons achieve sufficient range to reach them. However, he also notes that so long as the United States cannot significantly limit damage from Chinese and Russian retaliatory attacks, Washington will have very little incentive to use non-nuclear hypersonic weapons to launch a preemptive strike against either country.[68]

Strategic stability has been defined as a state of affairs in which countries are confident that adversaries cannot undermine their nuclear deterrent capability.[69] It implies that strategic stability would be shaken if emerging technologies threaten the survivability of nuclear deterrent capability (second-strike capability). Fearing a disarming first strike by an adversary that uses emerging technologies, nuclear-armed states might attempt to use nuclear weapons first before losing their second-strike capability in an attack. In other words, if a state perceives that its second-strike capability will become vulnerable, it will feel compelled to use its nuclear forces early, thereby increasing the incentive for a first strike in a crisis. Matthew Kroenig from Georgetown University, while warning against overemphasizing this logic of "use it or lose it," analyzes that the continued spread of emerging technologies to revisionist states like China and Russia could increase the risk of non-nuclear (conventional) war, and by extension, lead to nuclear escalation that can undermine strategic stability. Conversely, he suggests that emerging technologies will reinforce existing strategic stability for status quo powers, including the United States.[70]

Quantum technology too may make second-strike capabilities vulnerable. As mentioned, if quantum sensors facilitate the detection and tracking of SSBNs, their invulnerability will be significantly compromised, which will destabilize nuclear deterrence. It has also been suggested that if quantum technology is combined with AI and AI is enhanced by quantum computing, hypersonic weapons will become even more difficult to intercept.[71]

Due to the integration of AI into the cyber domain, cyber attacks may make SSBNs increasingly vulnerable. James Johnson from the Department of Politics and International Relations at the University of Aberdeen warns that conducting autonomous attacks by using AI in advanced persistent threat (APT) operations, a type of cyber attack, may enable the attacker

to rapidly identify and penetrate security weaknesses, even against highly secure targets such as SSBNs. He states that such opportunities for attack could arise when SSBNs are docked for maintenance.[72]

Given the heightening risk that new domains and emerging technologies will increase the vulnerability of second-strike capabilities, measures are needed to enhance the resilience of such capabilities to establish deterrence by denial, that is, dissuading adversaries from attacking by creating a posture that checks an attack on second-strike capabilities and making adversaries think that their objectives of attack are unattainable. In particular, NC3 systems' vulnerability to attacks in new domains makes it a matter of urgency to strengthen the deterrence by denial posture. Michael Gleason from The Aerospace Corporation and Peter Hays argue that deterrence should be strengthened by enhancing the resilience of space assets, thereby deterring adversaries from attacking. Suggested measures to reinforce resilience include deploying decoy satellites and escort assets and increasing the number of satellites.[73]

However, strengthening deterrence by denial against attacks on NC3 has limitations. Methods for defending satellites from attacks generally include satellite hardening, enhanced maneuver, and deployment of escort assets in orbit. Among these, hardening and maneuver are in a trade-off relationship with satellite performance (such as surveillance and communication capabilities) and design lifespan. Since maximizing performance is usually prioritized in satellite design, self-defense features must be curtailed. Moreover, deploying escort assets is technically challenging as of date.[74] Therefore, there are technical limitations to strengthening deterrence by denial against anti-satellite attacks in space.

Deterrence by denial against cyber attacks on NC3 is also challenging in reality. Generally, deterrence by denial can be strengthened to some extent if the defender improves the cybersecurity of the targeted system, increasing the cost of attacks and making the attacker think that the gains from the attack are not worth the cost. However, improving cybersecurity entails significant human, technical, and financial costs. Conversely, an attacker only needs to find and penetrate security weaknesses in the target system. If the defender notices penetration and fixes

The threat of cyber attacks is increasing (Jonathan Raa/NurPhoto/Kyodo News Images)

the weakness, the attacker simply needs to look for other weaknesses. Therefore, attacks are inexpensive. No matter how much the defender invests, it is impossible to discover and fix all security weaknesses in the system in advance.[75] While NC3 systems are required to have the highest level of cybersecurity, all security weaknesses cannot be eliminated. The U.S. Congress has passed a succession of legislation in a short time span, calling on the Department of Defense to take necessary measures to enhance the cybersecurity of the NC3 system.[76] However, improving the cybersecurity of NC3 is expected to be even more costly than that of other weapons systems, raising doubts about whether the security level of NC3 can be elevated sufficiently to impose costs on the attacker that exceed the potential gains from a cyber attack on NC3 and decrease the incentive for attack.

The Effectiveness of Deterrence by Punishment against Attacks in New Domains

The increasing vulnerability of second-strike capabilities due to new domains and emerging technologies, as examined in the previous section, makes the deterred country less convinced that an attack would be met with retaliation and reduces the effectiveness of deterrence by punishment. For deterrence by punishment to be effective, the deterring country must be able to identify the deterred country, the origin of attack. However, in attacks in new domains, identifying the origin itself is challenging. In the space domain, the coverage of space surveillance radars and telescopes used to observe orbital objects has many blind spots.[77] Therefore, even if some kind of attack on a satellite occurs, it is difficult to obtain detailed information to identify the origin. Sensor detection and information tracking can be used to determine the launch location of a direct-ascent anti-satellite missile and to identify the country that fired it. However, in the case of anti-satellite attacks using laser weapons or electronic warfare, detection and tracking are difficult, making it immensely challenging to identify the origin.[78] In the cyberspace domain, it can take several months to collect sufficient evidence to identify the origin of a cyber attack, resulting in the loss of a timely opportunity for effective response for deterrence.[79]

Even if the origin can be identified, it may be challenging in new domains to convince the attacker (the deterred country) that an attack will garner an unbearable retaliatory response. In the space domain, because attacking unmanned satellites does not result in human casualties, the attacker (the deterred country) may not necessarily be convinced that retaliatory actions would be taken. As already discussed, there are four categories of anti-satellite attacks: kinetic physical; nonkinetic physical; electronic; and cyber.

Specific attack options using these means are numerous and include those that cause either reversible temporary dysfunction or irreversible permanent damage. Having effective retaliatory means against all of these attacks is close to impossible, making it difficult for the deterring country to issue clear, specific, and credible deterrence threats against each attack. Accordingly, deterrence by punishment becomes uncertain, giving the adversary an incentive to attack. For example, adversaries may attempt a nonkinetic attack to test the deterring country's willingness to retaliate. Allowing such attacks itself would mean a failure of deterrence.[80]

In that case, should anti-satellite attack capabilities for retaliation in the space domain be deployed in orbit for similar retaliatory actions? The answer is that this would be challenging, as it would trigger an international arms buildup for deploying anti-satellite attack systems in space. Former U.S. Ambassador to Jordan Roger Harrison and others indicate that limiting U.S. responses to anti-satellite attacks to similar retaliation in space would be disadvantageous for deterrence. They posit that making the attacker believe that it cannot rule out a disproportionate response in other domains would mitigate the destabilization of deterrence.[81]

In the cyberspace domain, even if the origin of a cyber attack can be identified, it is technologically challenging to retaliate against the attacker's (the deterred country's) network system using similar cyber capabilities. If the deterring country threatens cyber retaliation, it could lead to the leakage of technological information, giving the deterred country an opportunity to fix vulnerabilities in its network system. In addition, if the deterred country becomes aware that a retaliatory Distributed Denial of Service (DDoS) attack is imminent, it can take countermeasures, such as taking critical systems to be protected off the network or redirecting harmful network traffic, and make the retaliation ineffective. While retaliation by zero-day attacks, which exploit unknown and unpatched vulnerabilities, might initially be effective, their effectiveness diminishes once the retaliation is carried out and the deterred country discovers the vulnerabilities and applies patches.[82]

Nuclear retaliation against a cyber attack would gain credibility if the attack was serious enough to incapacitate key nuclear weapons systems, including the U.S. NC3.[83] In this respect, the threat of nuclear retaliation may be able to deter cyber attacks. However, if the attacker deems that the threat is highly disproportionate and is not very credible, the deterrent capability of nuclear weapons may be undermined. Additionally, there is the issue of what would happen if nuclear threat fails to deter and a cyber attack is conducted. It should be kept in mind that decisionmakers will be under increasing psychological pressure to order the use of nuclear weapons to rebut domestic criticisms over a weak response to a cyber attack on NC3

and to shore up international perceptions about the credibility of nuclear threats, which may increase the risk of escalation to nuclear conflict.[84]

Heightened Possibility of Unintended Nuclear Use

There is a heightening possibility that attacks in new domains will lead to unintended escalation, or that a misunderstanding by the attacked country will evolve into the use of nuclear weapons. Notably, the United States, China, and Russia are enhancing their anti-space and cyber attack capabilities that could target each other's NC3 systems. The three countries have a shared recognition that a surprise attack using these capabilities on their NC3 systems would undermine strategic stability. In an international crisis, their militaries are anticipated to intensify monitoring, determined to detect signs of attack against their nuclear weapons systems. If a local conventional war involving the three countries were to occur in these circumstances, they will conceivably try to turn conventional operations to their advantage by using anti-space or cyber capabilities to strike the C3 systems supporting the adversary's conventional operations. However, the U.S., Chinese, and Russian C3 systems used for conventional operations are often also used for NC3.[85] Therefore, even if they intentionally exclude NC3 systems and attempt to attack only C3 systems for conventional operations, they are inadvertently attacking NC3 systems, increasing the risk of nuclear escalation. For example, it is unclear which U.S. military satellites supporting NC3 are for NC3 or for conventional operations.[86]

The possibility of nuclear-armed states' second-strike capabilities becoming vulnerable to attacks in new domains also heightens the risk of unintended use of nuclear weapons. James Acton notes that the vulnerability of nuclear weapons systems to cyber attacks creates the risk of inadvertent nuclear escalation. Such risks can be triggered by both counterforce cyber attacks aimed directly at nuclear weapons systems, and cyber espionage intended to steal information from these systems. Even if the attacked country assessed that the cyber activity was intended for information theft, it will be of concern to the country that the information collected by the activity could be used for a counterforce strike against it. As cyber espionage and regular cyber attacks cannot be distinguished quickly, there is a high risk that cyber espionage targeting nuclear weapons systems will be mistaken for a counterforce cyber attack.[87] In particular, if NC3 is subject to a cyber attack, the attacked country will feel pressured to escalate the conflict and use nuclear weapons before its nuclear weapons system is incapcitated,[88] making inadvertent nuclear escalation more likely.

In warfare in the cognitive domain, the U.S. forces are facing the threat

of "neuro-strike" weapons,[89] which could destabilize nuclear deterrence. The effects of such weapons' attacks on the human body are apt to be mistaken for mere health issues. For this reason, detecting attacks is difficult, and deterrence is thought to be ineffective.[90] A nuclear-armed state with access to neuro-strike weapons may attempt to use them to influence the nuclear decisions of decision-makers and create a favorable situation for itself. However, neuro-strike weapons have a limited effective range, making targeting decision-makers seemingly challenging. Even if it were possible, a state cannot control their cognition to its liking. This has the high risk of generating unintended decisions and breaking down nuclear deterrence.

There is concern that the use of emerging technologies in nuclear weapons systems will exacerbate the risk of unintended nuclear use due to misunderstandings, misidentifications, miscalculations, or accidents.[91] This concern heightened as Russia's unmanned underwater nuclear weapon development project, which Moscow calls the "Oceanic Multipurpose System Status-6," became known to the world and as observers analyzed that AI would be applied to the weapon.[92] If AI technology is actually employed by this unmanned nuclear weapon, later named "Poseidon," predictability during a crisis could decrease, increasing the risk of misunderstanding the adversary's intentions.[93]

Poseidon is an example of AI's application in nuclear weapons themselves. A more serious concern for the destabilization of nuclear deterrence is the integration of AI into NC3. AI is expected to be used in four areas of NC3: communication; early warning systems; decision support; and automated retaliatory attacks.[94] Especially controversial among them are decision support and automated retaliatory attacks. In the case of decision support, there is concern that AI could result in unintended actions, increasing the risk of accidental escalation to nuclear war.[95] An example of automated retaliatory attacks is the automated nuclear retaliation system that Russia reportedly developed during the Soviet era. This system was developed for a scenario in which a nuclear attack wipes out Russia's leadership. Sensors detect signs of a nuclear explosion, such as seismic waves, and if the survival of senior officials cannot be confirmed, it launches a semi-automatic nuclear missile retaliatory attack.[96] According to Anthony Barrett from RAND Corporation, the sensors of Russia's automated nuclear retaliation system may mistake a meteorite strike for a U.S. nuclear attack, potentially leading to unintended nuclear use.[97]

Furthermore, if attacks in the cognitive domain impact AI used in NC3, the risk of unintended nuclear escalation could increase. For example, as AI algorithms accelerate the progression of conflicts, the AI systems of nuclear-armed states may be distorted by disinformation, potentially

causing unintended escalation. Therefore, it has been suggested that technical measures to identify disinformation, deep-fakes, and intentionally manipulated data should be researched, assuming that AI used in NC3 may be corrupted by such data.[98]

In view of the assortment of issues that come with the use of AI in NC3, there have been discussions about taking all possible operational and technical measures for applying AI, or discussions about deferring the use of AI. Peter Rautenbach, a scholar well-versed in this issue, argues that to prevent AI-attributed accidental nuclear use, it is necessary to not only ensure human intervention in AI decisions (humans in the loop), but also implement feasible technical solutions and rigorous technical reviews when integrating AI into NC3. Moreover, he calls for fundamental nuclear operation measures, such as altering the nuclear doctrine and policy.[99] Additionally, Alice Sartini from the European Leadership Network describes that AI's integration into NC3 is technically premature and that a moratorium on the integration is needed. She suggests that the P5 (United States, United Kingdom, France, China, and Russia) begin discussions to realize this moratorium, and that it would be desirable to eventually include other nuclear-armed states, such as India and Pakistan, in these discussions and have all nuclear-armed states agree to the moratorium.[100]

Future Challenges and Prospects

Policy Challenges Facing New Domains' Destabilization of Nuclear Deterrence

The preceding sections discussed that the link between new domains and nuclear weapons systems can stabilize, but at the same time, may also destabilize nuclear deterrence. The possibility of the former is examined in a little more detail below.

Attacks in the space, cyberspace, and electromagnetic domains and attacks on NC3 in particular have a high potential to provoke nuclear retaliation. Therefore, it is conceivable that states will mutually restrain from attacks. However, this mutual restraint is in no way easy.

Deterrence threats are perceived as credible if they are deemed proportionate to the action a state seeks to deter. In this context, threatening nuclear retaliation to deter cyber espionage against NC3 will not be deemed credible in all likelihood.[101]

Yet, a country intending to attack (deterred country) cannot be certain that the opponent will necessarily limit its response to proportional

retaliation. For example, if the U.S. response to an anti-satellite attack in space were limited to retaliation of the same scale, the United States would seemingly have a deterrence disadvantage. Thus, the attacking country must consider the possibility of the United States responding to its attack with a disproportionate retaliatory action, leading to rapid escalation.[102] This implies that mutual tension will increase during a crisis, facilitating escalation. Whether this situation will manifest or not would depend on the level of communication between the opponent and the deterred country regarding new domains.

The use of the cognitive domain to deter nuclear use, particularly "cognitive targeting," will be unsuccessful if the opponent sees through the strategy of one's country. In such cases, the opponent will try to induce cognitive biases to mislead its actions, or sow doubt about the responses of one's country to make its deterrence strategy fail. For example, the opponent may foster an optimism bias, making one's country believe that its deterrence strategy is working effectively, or by contrast, spread disinformation suggesting that deterrence is already partially failing and causing confusion.[103] If so, the opponent could gain the upper hand in the warfare in the cognitive domain. If rationalistic thinking is distorted through the dissemination of disinformation or other cognitive manipulations by the opponent, the risk of nuclear deterrence failure increases.

Lastly, using emerging technologies to contain the use of nuclear weapons is thought to restrain nuclear-armed states that were first to adopt such technologies. However, if these technologies become widespread and the opponent also adopts them, it could, on the contrary, lead to the destabilization of nuclear deterrence. For example, the integration of AI into NC3 might provide decision-makers with more time to make nuclear decisions. However, if not only one's country but also the opponent adopt AI, AI would shorten the decision-making time for both countries, which in turn will further accelerate the progression of the situation.[104]

While the link between new domains and nuclear weapons systems may stabilize nuclear deterrence, the above suggests that it depends on the relationship or level of communication between the deterring and the deterred countries in new domains. It should be noted that the actions of the deterred country could, conversely, lead to destabilization of nuclear deterrence.

In sum, the link between new domains and nuclear weapons systems makes the destabilization of nuclear deterrence highly likely. In view of this, the policy challenges for stabilizing deterrence are considered next.

First, the parties need to have a shared perception about deterrence in new domains. Efforts to establish mutual understanding on what activities

are acceptable or unacceptable in new domains will be especially crucial. When there still lacks sufficient mutual understanding, there is a potential for some countries to seek to justify highly destructive attacks, for example, in the cyberspace domain. Furthermore, because the parties tend to have a vague and unclear understanding of what constitutes acceptable cyber attacks, unintended accidental escalation can occur. Moreover, extended competition with each other in new domains may result in shifts in countries' relative power, destabilizing power relations and potentially leading to armed conflict.[105] For this reason, Vincent Manzo from the U.S. National Defense University argues that a shared framework with potential adversaries is needed to determine what types of attacks can ensure proportionality in new domains and which attacks are escalatory.[106]

At the same time, it is also important not to rule out the possibility of disproportionate retaliation from the outset. Even if retaliation or retaliatory threat based on the principle of proportionality is invoked in response to an attack in new domains, it is considered to have a limited deterrence effect, making it difficult to prevent escalation if the attack is not deterred. For example, if an electronic attack temporarily disables a satellite, even a proportionate response, such as launching an electronic attack in retaliation against the attacker's satellite after identifying the origin of attack, may be able to prevent escalation. However, if the attacker deems that the opponent will carry out only retaliation based on the principle of proportionality, deterrence in new domains becomes difficult. Thus, reserving the possibility of disproportionate retaliation is desirable from a deterrence policy perspective. In this context, it is necessary to consider under what terms and conditions the credibility of disproportionate retaliation can be enhanced. Another policy challenge is aligning this with the principle of proportionality under international humanitarian law.

Additionally, from a CDD perspective, it is desirable to use non-nuclear threats in one domain to prevent attacks on nuclear weapons systems in another domain. For example, using threats in the cognitive domain may be considered in order to deter attacks on NC3 space assets. Generally, authoritarian states hostile to the United States and other democratic countries will try to disseminate a government-created political narrative through domestic mass media and prevent the widespread circulation of facts that contradict this narrative. In this respect, if these authoritarian states attempt to attack U.S. NC3 space assets, an effective way to deter the attack may be to broadcast a 24-hour satellite news program that directly reaches the citizens of authoritarian states, reporting facts that contradict their political narrative, undermining public support and threatening the survival of authoritarian regimes.[107] However, a careful review is needed to determine whether the use of such threats is appropriate under democratic norms.

Continuous monitoring of the emergence of threats in new domains and the establishment of a system to swiftly detect threats to NC3 are also key policy challenges. The U.S. forces have already set up a monitoring system for the space and cyberspace domains and conduct ongoing space situational awareness (SSA) and cyberspace surveillance. However, the system cannot detect all threats to NC3. With regard to SSA, capabilities have improved for monitoring space objects, such as space debris, and avoiding their collisions with satellites, making it possible to detect physical attacks against satellites to some extent. However, detecting non-physical attacks likely remains challenging. In the cyberspace domain, despite advances in forensic technologies against cyberattacks, forensic capabilities are limited by cyber attack techniques that are constantly evolving.[108] Overcoming these challenges is expected to incur significant costs, but they should be considered a necessary investment to swiftly detect various threats to NC3 in new domains and prevent the destabilization of nuclear deterrence.

In order to counter the destabilization of nuclear deterrence, steps must be taken to increase NC3's resilience. The United States recognizes that the modernization of NC3 requires greater resilience especially against EMP and cyber threats.[109] The U.S. NC3 system is said to fulfill the functions of: (1) attack detection, warning, and characterization; (2) nuclear planning; (3) decision-making conferencing; (4) receiving presidential orders; and (5) the management and direction of nuclear forces.[110] Function (1) includes the Next Generation Overhead Persistent Infrared (OPIR) program that is under way to modernize the existing Space-Based Infrared System (SBIRS) early warning system.[111] Function (2) includes plans to update the software of the existing Integrated Strategic Planning and Analysis Network (ISPAN).[112] Additionally, E-4B's EMP hardening is being considered for modernizing the E-4B National Airborne Operations Center (NAOC), which conducts command operations from the air in the event that an NC3 ground command center is destroyed.[113] As regards cyber measures, Northrop Grumman, which has been contracted to develop the next generation OPIR satellites, is working on creating a system that can withstand cyber attacks, according to the company.[114] The overall plan for the modernization of the U.S. NC3 has not been disclosed, and improvements in the resilience of NC3 need continued attention and monitoring.

Extended Nuclear Deterrence in New Domains and the Role of Umbrella States

The previous section considered the policy challenges for stabilizing nuclear deterrence if it were destabilized by new domains. This consideration assumed direct deterrence by nuclear-armed states, in other words, deterring an attack on one's own state. In this section, extended deterrence, or deterring an attack on an ally of nuclear-armed states, is examined.

Specifically, this discussion focuses on countries under the U.S. extended nuclear deterrence called a "nuclear umbrella." It examines the role that these umbrella states should play in stabilizing U.S. extended nuclear deterrence if it were destabilized by new domains and emerging technologies.

Attacks in the space, cyberspace, and electromagnetic domains are not necessarily targeted at the United States. They may very well be directed at umbrella states. In such cases, Washington would face the dilemma of whether it should engage in retaliation against the attacker when the United States itself was not attacked. Dean Cheng from the Heritage Foundation raises the questions of whether the United States should jam the space assets of the attacker in retaliation for its jamming or other non-physical attacks on U.S. allies' space assets, or what proportional retaliation the United States could take against the attacker if it launched a cyber attack on U.S. allies' command and control networks.[115] If the United States does not retaliate or otherwise respond appropriately to attacks directed at umbrella states, their trust in the U.S. commitment is expected to decline, destabilizing the extended nuclear deterrence.

To prevent this situation, what role should umbrella states play? Using the case of the U.S.-Republic of Korea (ROK) alliance, scenarios in which North Korea launches a cyber attack on the ROK, an umbrella state, are examined. Cyber attacks that the U.S.-ROK alliance should deter and respond to are deemed to be major attacks that have strategic-level effects, such as attacks targeting the ROK's critical infrastructure or military command and control networks. James Platte of the U.S. Air Force lists five North Korean cyber attacks: (1) a large-scale DDoS attack on ROK government and other websites in July 2009; (2) a cyber attack on the ROK financial system in April 2011; (3) cyber attacks on ROK media, banks, and the Blue House in March and June 2013; (4) hacking of an ROK nuclear power plant in December 2014, leading to the leakage of a nuclear power plant blueprint and other data; and (5) a cyber attack on the ROK defense network in September 2016, resulting in the leakage of U.S.-ROK confidential information. Platte identifies (4) and (5) as major cyber attacks that should be deterred by the alliance. The reason is that, while (4) and (5) did not have significant strategic-level effects on the United States and the ROK, any similar incident in the future could cause serious consequences. He suggests that the ROK independently respond to the remaining types of cyber attacks.[116] The alliance cannot deter and respond to all incidents from (1) to (5). Thus, if the alliance deters strategic-level cyber attacks and the ROK responds to lower-level attacks, it would clarify the alliance's deterrence focus and the role the ROK should play in handling cyber attacks. However, distinguishing between cyber attacks that have major strategic-level effects and lower-level attacks is difficult in reality. The extent of the effect can only be assessed after deterrence fails and an attack occurs, and therefore, the appropriateness of making assessments in advance should be considered.

Attacks in the cognitive domain may also be directed at umbrella states as part of a policy to divide the alliance. For example, China or Russia may use disinformation to conduct influence campaigns against umbrella states in order to sow doubt among them about the continuity of the U.S. extended deterrence commitment. If successful, this could make it difficult to coordinate joint deterrence actions with the United States, and could foster disagreements with the United States over the combination of nuclear, non-nuclear, and non-kinetic capabilities that the alliance needs.[117] To prevent these scenarios from becoming a reality, umbrella states need to increase their citizens' resilience to influence campaigns. The North Atlantic Treaty Organization (NATO) suggests that cognitive warfare using social media may be conducted against the people of NATO member states, including umbrella states. To counter such warfare, NATO discusses the importance of deepening member states' understanding of cognitive warfare and increasing their people's resilience to campaigns that seek to exploit the openness of democratic states and divide civil society.[118] Such cognitive warfare could be aimed at shaking umbrella states' trust in the U.S. extended deterrence policy and in decision-making processes of NC3. Accordingly, increasing the resilience of umbrella states plays a crucial role in preventing the destabilization of nuclear deterrence.

Umbrella states also have an important role to play in fostering a shared recognition with the United States on emerging technologies' potential to destabilize nuclear deterrence. For example, it would be desirable for umbrella states and the United States to discuss and align their perceptions on what would happen to the decision-making processes of NC3 if AI is used as an NC3 decision-making tool, or whether this would destabilize nuclear deterrence. Additionally, discussion is needed on the nuclear deterrence challenges that may arise if AI is integrated into systems supporting non-nuclear operations, rather than NC3, and these systems are connected

to NC3. Currently, the United States is pushing the Joint All Domain Command and Control (JADC2) concept, which aims to connect all military sensors and shooters in real-time for combat. At this point, JADC2 does not refer to specific networks or systems but rather a strategy for a new U.S. forces command and control approach.[119] If the JADC2 concept eventually converges into a concrete system in the future, it will likely be used to command and control U.S. forces' non-nuclear capabilities. AI may be integrated into the JADC2 system, and it cannot be ruled out that this system will be connected to NC3.[120] Irrespective of this possibility, JADC2, as its name implies, is understood as aiming to increase the U.S. forces' operational capabilities, including in new domains. If AI is integrated into JADC2, it is expected to impact nuclear deterrence. As mentioned earlier, C3 systems for non-nuclear operations are already dual-used with NC3. Therefore, the integration of AI into the JADC2 system should be understood as also potentially affecting NC3. Taking this into consideration, umbrella states should deepen their discussions with the United States regarding the nature of extended nuclear deterrence in new domains.

It is desirable that umbrella states pursue the extended nuclear deterrence agenda relating to new domains and emerging technologies and reflect it into the alliance's nuclear policy. Umbrella states participate in two NATO nuclear sharing arrangements: nuclear weapons sharing by some of the member states; and the nuclear consultation of NATO's Nuclear Planning Group (NPG), which is participated by almost all member states. Umbrella states are anticipated to raise the agenda in both policy frameworks.

NATO's nuclear weapons sharing involves the United States pre-deploying B61 tactical nuclear bombs in five of NATO's umbrella member states: Belgium; Germany; Italy; the Netherlands; and Turkey. In the event of a contingency, the United States would provide B61 bombs to the five countries with the president's authorization. These countries, in turn, use the B61 bombs carried on dual-capable aircraft (DCA) for conventional and nuclear weapons.[121] Alexander Mattelaer from the VUB Brussels School of Governance suggests that NATO's nuclear sharing arrangements be reviewed from the perspective of CDD and ensure their quick adaptation to the changing security environment. He argues that it is desirable to proceed with the replacement of DCA with the F-35 stealth fighter and the modernization of the B61.[122] Regarding the modernization of the B61, plans are under way to deploy to Europe the B61-12 with higher hit accuracy, which, along with the replacement of DCA with the F-35, is expected to enhance NATO's localized deterrence capability.[123] While the U.S. Department of Defense announced in October 2023 that it would develop a new B61-13 model of the B61 series,[124] it is unclear at this time whether the B61-13 will be developed as a bomb compatible with fighters and if it will be deployed in Europe for use as a nuclear bomb carried on DCAs.[125]

In parallel with the modernization of nuclear capabilities, it is desirable that NATO's umbrella states raise in the NPG and other forums the issues related to NATO's extended nuclear deterrence and nuclear sharing arrangements in new domains, and discuss policy prescriptions to prevent the destabilization of extended nuclear deterrence.

Although the Indo-Pacific region lacks a framework like NATO's nuclear sharing arrangements, in bilateral alliance nuclear discussions with the United States, umbrella states can still advocate for extended nuclear deterrence in new domains. In addition to intergovernmental consultations, it would be meaningful for umbrella states to utilize the Track 1.5 dialogue involving government officials and private-sector experts to raise an agenda for the threats in new domains and the challenges of extended deterrence in the Indo-Pacific region.[126]

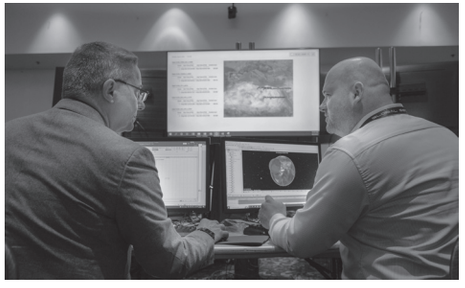
Expectations and Prospects for Arms Control

In recent years, there has been a growing call among experts for arms control in new domains. Victoria Samson and Brian Weeden from the Secure World Foundation urge the United States to take the lead in proposing legally binding measures to enhance the security and stability of space, including space arms control.[127] Gabriel Molini from The Catholic University of America argues that the international community should give top priority to regulating cyber attack capabilities, due to concerns that retaliation for attacks in cyberspace may escalate inter-state tensions and result in severe consequences, especially if nuclear-armed states are involved.[128] As has been discussed, since the link between new domains and nuclear weapons systems could destabilize nuclear deterrence, arms control measures will be needed to ensure stable relations between nuclear-armed states.

The arms control agenda for new domains and nuclear weapons systems is examined below, beginning with arms control in the space domain.

As already reviewed, offensive anti-satellite capabilities pose a threat to the space assets of NC3. Therefore, to prevent the destabilization of nuclear deterrence, regulation of such capabilities is considered the focus of arms control efforts in the space domain. In this connection, China and Russia have stood firm on aiming for a legally binding arms control treaty, and they jointly submitted a draft Treaty on the Prevention of the Placement of Weapons in Outer Space and of the Threat or Use of Force against Outer Space Objects (PPWT) in 2008. Negotiations on the draft PPWT have not

commenced for reasons including verification difficulties and the treaty's exclusion of ground-based anti-satellite weapons. In contrast to the Chinese and Russian treaty-based approach, the United States and other Western countries believe that the greatest threats to space security are not specific weapons but behavior and actions in orbit, and adopt an approach that aims to establish norms for responsible behavior and actions in space.[129] Underlying the West's pursuit of a code of conduct approach is the recognition that, due to the difficultness of defining what constitutes "weapons" in space, it is ineffective to apply the traditional arms control approach sought by China and Russia, which is aimed at regulating and controlling specific weapons, making verifications de facto impossible. For example, rendezvous and proximity operations (RPO), which involve approaching satellites in orbit for refueling or repairing, too can be used to make a precise approach and destroy targeted satellites.[130] That said, regulating space assets capable of RPO as "weapons" would not only be meaningless but could also hinder essential satellite maintenance operations. Yet, the code of conduct approach also has limitations. It is difficult to distinguish between satellite jamming and noise caused by unintended radio interference. Furthermore, it is challenging to identify the origin of cyber attacks on satellites, and it is not easy to track and trace the origin of laser attacks on satellites. Consequently, the offender can deny its behavior and actions,[131] making verification and ensuring transparency challenging.



Anti-satellite weapon simulation exercise (John Ayre/U.S. Space/Planet Pix via ZUMA Press Wire/Kyodo News Images)

Despite these limitations, the code of conduct approach may still be able to reduce the threat of offensive anti-satellite capabilities to NC3 space assets to some extent. In particular, it may be possible to reach an international agreement on refraining from attacking NC3 space assets. If aiming for an international agreement from the outset is challenging, it would be desirable to start with unilateral restraint, followed by informal agreements, and gradually form an international consensus.[132] In the area of arms control in the space domain, the United Nations General Assembly adopted a resolution on "Reducing Space Threats through Norms, Rules and Principles of Responsible Behaviors" in December 2020, and the first meeting of the United Nations working group based on this resolution was held in Geneva in May 2022.[133] It is expected that these international efforts will lead to an agreement on refraining from attacks on NC3 space assets and contribute to preventing the destabilization of nuclear deterrence.

Next, arms control in cyberspace is examined. Defining "weapons" is as challenging in cyberspace as it is in space, and a traditional arms control approach may not be able to guarantee effectiveness or transparency. Andrew Futter from the University of Leicester suggests that it might be more significant to regulate the targets or actions of cyber attacks rather than "cyber weapons," which are intangible unlike ordinary weapons, and therefore, difficult to control.[134] From this perspective, instead of prohibiting or regulating intangible "cyber weapons" on the whole, it would be meaningful for arms control to limit regulations to elements that destabilize nuclear deterrence, such as regulating cyber attacks targeting NC3. As a specific option, Heather Williams and Nicholas Smith Adamopoulos from the Center for Strategic and International Studies give the example of an informal agreement among the United States, China, and Russia to refrain from cyber attacks on each other's NC3 following the Russo-Ukrainian War.[135]

As for arms control in the electromagnetic domain, directed-energy weapons could potentially disable nuclear weapons systems at or below the theater level, as noted by Anderson and McCue. In view of this, it is desirable to consider frameworks that regulate the use of directed-energy weapons against these systems. Namely, the U.S. B61-12 tactical nuclear bombs, which are being deployed in five NATO member states, are equipped with an inertial navigation system to increase the hit accuracy[136] and could be affected by directed-energy weapons. If so, the above frameworks are believed to contribute to the stabilization of NATO's nuclear deterrence. However, instead of a traditional arms control approach that regulates directed-energy weapons themselves, it would be preferable to pursue a normative approach that outlines actions that should be avoided for stabilizing nuclear deterrence, with the use of directed-energy weapons that could destabilize nuclear deterrence being among the regulated actions. The normative approach is also relevant to issues in the cognitive domain which are explored below.

While the arms control agenda in the cognitive domain overlaps with that in the electromagnetic domain, the former also requires consideration of regulating attacks that use directed-energy weapons targeting the human brain. As mentioned earlier, weapons that use the electromagnetic environment to directly attack the human brain are reportedly beginning to be developed. If such weapons and attack methods become more advanced, attacks may also be targeted at personnel involved in nuclear

weapons systems. If a nuclear decision-maker were attacked, it cannot be ruled out that their judgment and decisions would be adversely affected, destabilizing nuclear deterrence. Accordingly, neuro-strike weapons could incentivize preemptive strikes in a crisis and potentially increase the risk of war. Therefore, observers point to an urgent need for arms control efforts to regulate these weapons.[137]

In light of the nuclear deterrence risks of integrating emerging technologies into NC3, scholars have noted the need for arms control to regulate these technologies. Lauren Kahn from the Council on Foreign Relations contends that AI has not yet reached the level of technical maturity for nuclear-armed states to confidently integrate it into NC3, and therefore, nuclear-armed states should quickly reach an agreement to regulate the use of AI that could destabilize nuclear deterrence and increase the possibility of nuclear use.[138] Again, instead of the traditional arms control approach of regulating AI as a "weapon," a major step toward the future would be to pursue a normative approach under which the use of AI that could destabilize nuclear deterrence would be considered an "action" that should be avoided. In this vein, some have noted that cyber attacks on AI-enabled nuclear weapons systems may alter the AI's training data and disable the adversary's nuclear weapons system.[139] While envisaging such possibilities, another question to be considered is whether the specific "action" of a cyber attack targeting AI used in a nuclear weapons system is an action that should be avoided.

In contrast, the regulation of hypersonic weapons may lend itself to a traditional arms control approach. Spenser Warren states that it would be desirable for the United States to propose Russia with limiting hypersonic weapons to advance strategic nuclear weapons reduction negotiations to its favor and re-establish limits on intermediate-range nuclear forces, paving the way for a nuclear arms control agreement between the United States and Russia and eventually bringing China into the agreement.[140] However, it should be noted that in such negotiations, China and Russia are likely to demand the U.S. missile defense system's inclusion in the regulation. Faced with superior U.S. missile defense capabilities, China and Russia initially began developing hypersonic weapons to secure second-strike capabilities for avoiding the missile defense system and conducting retaliatory attacks. In this sense, China and Russia might find greater benefit from the United States' missile defense regulation, even in exchange for regulation on hypersonic weapons. Therefore, if the regulation of hypersonic weapons becomes part of the future U.S.-Russia(-China) arms control agenda, it is expected to be discussed in conjunction with the regulation of the U.S. missile defense system.

Some suggest that agreements for regulating emerging technologies may be easier than regulating already established weapons technologies.[141] In 2020, Russia actually proposed that it was ready to include the Avangard newly developed hypersonic glide vehicle and the new Sarmat ICBM under the regulations of the New Strategic Arms Reduction Treaty (New START) in exchange for extending the treaty.[142]

In addition to simply regulating emerging technologies, it is also worth considering their use in a way that would benefit arms control. The potential application of AI for arms control verification has already been discussed. Another possibility is using quantum technology to monitor nuclear weapons and enhance verification of compliance with arms control agreements. Hayes suggests that it would be desirable for arms control purposes to establish an independent, impartial early warning fusion center that can use quantum technology to obtain monitoring and verification data, based on which appropriate advice would be provided to nuclear-armed states.[143]

Conclusion

This chapter examined how operations in new domains, namely space, cyberspace, electromagnetic, and cognitive domains, are linked to and impact nuclear weapons systems. It focused on the question of whether the link between new domains and nuclear weapons systems stabilizes or destabilizes nuclear deterrence. This analysis assumed that emerging technologies, which act as enablers of operations in new domains in the way that AI enhances offensive cyber capabilities, have significant influence on new domain dynamics. To explore if the link between new domains and nuclear weapons systems stabilizes nuclear deterrence, this study considered mutual restraint of attacks in space and cyberspace, the use of the cognitive domain to deter the use of nuclear weapons, and the application of emerging technologies to suppress nuclear use. It was noted that the possibility of each is influenced by the relationship or level of communication on new domains between deterring and deterred countries, and that nuclear deterrence may be destabilized depending on the actions of the deterred country. The deterrence destabilization risks identified were: the increasing vulnerability of second-strike capabilities in new domains; the issue of the effectiveness of deterrence by retaliation against attacks in new domains; and the increasing likelihood of unintended use of nuclear weapons. It concluded that the link between new domains and nuclear weapons systems is likely to destabilize nuclear deterrence.

In view of this, this chapter discussed (1) policy challenges facing the

destabilization of nuclear deterrence by new domains, (2) extended nuclear deterrence in new domains and the role of umbrella states, and (3) the expectations and prospects for arms control. (1) revealed the following policy challenges with U.S. direct deterrence in mind: parties having a shared perception about deterrence in new domains; retaining the possibility of disproportionate retaliation; leveraging CDD threats; establishing surveillance systems for new domains; and increasing the resilience of NC3. (2) discussed distinguishing between strategic-level attacks, which should be deterred by an alliance, and lower-level attacks, which umbrella states should handle independently; increasing the resilience of umbrella states to attacks in the cognitive domain; and umbrella states voicing the challenges of extended nuclear deterrence surrounding new domains and emerging technologies. Finally, (3) examined arms control in the space, cyberspace, electromagnetic, and cognitive domains, as well as the regulation of emerging technologies and their use for arms control. Notably, this chapter argued that traditional arms control approaches aimed at regulating and controlling specific weapons are ineffective for arms control in new domains and make verifications de facto impossible. It concluded that a major step toward the future would be to pursue a normative approach which regulates "actions" in new domains that could destabilize nuclear deterrence and outlines actions that should be avoided for stabilizing nuclear deterrence.

The link between new domains and nuclear weapons systems was examined. Rather than an exhaustive review of all conceivable scenarios, it no more than attempted to carry out an analysis based on a number of situations and issues currently being discussed among experts. Nevertheless, it is still possible to envision a near future where rapid advances in emerging technologies transform the space, cyberspace, electromagnetic, and cognitive domains that are now drawing increasing attention, further straining nuclear weapons systems and destabilizing nuclear deterrence. While nuclear weapons systems are also expected to be modernized to counter threats in new domains, the modernization of nuclear weapons systems is not a panacea. At least in the realm of cybersecurity, older analog systems are considered to be less vulnerable to cyber attacks than modern digital systems.[144] This envisioned near future anticipates the emergence of new domains that could have unknown effects on nuclear deterrence. In this sense, it is hoped that the issues surrounding new domains and nuclear weapons systems examined in this chapter will provide a glimpse into the "new horizons of the nuclear age."

1. King Mallory, "New Challenges in Cross-Domain Deterrence," *Perspective*, RAND Corporation (2018), 1.
2. The term cross-domain deterrence is considered to have first come into usage among U.S. defense officials in the late 2000s. Jon R. Lindsay and Erik Gartzke, eds., *Cross-Domain Deterrence: Strategy in an Era of Complexity* (New York: Oxford University Press, 2019), 4.
3. Tim Sweijs and Samo Zilincik, "Cross Domain Deterrence and Hybrid Conflict," Hague Centre for Strategic Studies (December 2019), 11-12. Regarding the concept of complex deterrence, see T. V. Paul, Patrick M. Morgan, and James J. Wirtz, eds., *Complex Deterrence: Strategy in the Global Age* (Chicago: University of Chicago Press, 2009).
4. All affiliations and titles of the people in this chapter are those as of the publication of their works.
5. Lindsay and Gartzke, *Cross-Domain Deterrence*, 6.
6. Sweijs and Zilincik, "Cross Domain Deterrence and Hybrid Conflict," 15-16.
7. 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), 11-12.
8. Vincent Boulanin et al., "Artificial Intelligence, Strategic Stability and Nuclear Risk," Stockholm International Peace Research Institute (June 2020), 105.
9. Tosaki Hirofumi, "Emerging Technologies and Nuclear Deterrence Relationship," English edition, The Japan Institute of International Affairs, April 26, 2021.
10. Marie Villarreal Dean, "U.S. Space-Based Nuclear Command and Control: A Guide," Center for Strategic and International Studies (January 2023), 1-5.
11. Don Snyder and Alexis A. Blanc, "Unraveling Entanglement: Policy Implications of Using Non-Dedicated Systems for Nuclear Command and Control," RAND Corporation (2023), 1-8.
12. Stephen M. McCall, "Space as a Warfighting Domain: Issues for Congress," *CRS in Focus*, no. IF 11895, Congressional Research Service (August 10, 2021).
13. Kari A. Bingen, Kaitlyn Johnson, and Makena Young, "Space Threat Assessment 2023," Center for Strategic and International Studies (April 2023), 4.
14. Ibid., 11-14.
15. Ed Browne, "Fact Check: Did Russia Use Lasers to Target Satellites over Ukraine Border?" *Newsweek*, October 5, 2022.
16. Bruce Blair, "Why Our Nuclear Weapons Can Be Hacked," *New York Times*, March 14, 2017.
17. Garrett K. Hogan, "The Electromagnetic Spectrum: The Cross Domain," Joint Air Power Competence Centre (November 2015).
18. Elżbieta Hodyr, "Cybersecurity of Nuclear Weapon Systems," *Cybersecurity and Law* 6, no. 2 (2021): 94-95.
19. Natasha Bertrand and Eric Wolff, "Nuclear Weapons Agency Breached amid Massive Cyber Onslaught," *Politico*, December 17, 2020.
20. "Russian Hackers Targeted US Nuclear Research Laboratories, Records

Reveal," *Guardian*, January 6, 2023.
21. Bishr Tabbaa, "Zer0 Days: How Stuxnet Disrupted the Iran Nuclear Program and Transformed Computer Security," *Medium*, July 17, 2020.
22. Kayla T. Matteucci, "Protecting Nuclear Command, Control, and Communications below the Threshold of Armed Conflict: Don't Count on Deterrence," Institute for Defense Analyses (June 2021), 31.
23. Juliana Suess, "Jamming and Cyber Attacks: How Space Is Being Targeted in Ukraine," RUSI, April 5, 2022.
24. Ariel Cohen, "Protecting America's Power Grids from EMP Attacks," *Forbes*, May 20, 2023.
25. Oriana Pawlyk, "Air Force Wants to Harden the B-2 Bomber to Withstand an EMP Attack," Military.com website.
26. "HiJENKS Missile: Bold Innovation from US Navy and Air Force Labs," SOFREP, July 7, 2022.
27. Peter Pry, "Non-Nuclear Electromagnetic Pulse (NNEMP) Attack on the U.S. Power Grid," Worldview Weekend Broadcast Network, June 21, 2021.
28. Theresa Hitchens, "Laser Weapons 'Finally' Seeing 'Real Progress,' Missile Defense Agency Official Says," *Breaking Defense*, August 17, 2023.
29. Justin Anderson and James R. McCue, "Deterring, Countering, and Defeating Conventional-Nuclear Integration," *Strategic Studies Quarterly* 15, no. 1 (Spring 2021): 48.
30. Mana Alahmad, "Strengths and Weaknesses of Cognitive Theory," *Budapest International Research and Critics Institute-Journal (BIRCI-Journal) Humanity and Social Sciences* 3, no. 3 (July 2020): 1584.
31. Bernard Claverie and François Du Cluzel, "'Cognitive Warfare': The Advent of the Concept of 'Cognitics' in the Field of Warfare," in *Cognitive Warfare: The Future of Cognitive Dominance*, Bernard Claverie et al., NATO Collaboration Support Office (2022), 2, 1-7.
32. Jean-Marc Rickli, Federico Mantellassi, and Gwyn Glasser, "Peace of Mind: Cognitive Warfare and the Governance of Subversion in the 21st Century," Policy Brief, Geneva Centre for Security Policy, August 25, 2023.
33. United States Senate Select Committee on Intelligence, "Report of the Select Committee on Intelligence United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election," vol. 1, 1-5.
34. Robert McCreight, "Neuro-Cognitive Warfare: Inflicting Strategic Impact via Non-Kinetic Threat," *Small Wars Journal*, September 16, 2022.
35. Sam Meyer, "Fake News, Real Consequences: The Dangers of WMD Disinformation," NTI, December 7, 2017.
36. Heather Williams and Alexi Drew, "Escalation by Tweet: Managing the New Nuclear Diplomacy," King's College London, July 2020.
37. Matty S. Golub, "Who's to Say?: Technical Dimensions of Nuclear Disinformation," *On the Horizon: A Collection of Papers from the Next Generation* (February 2021), 72-82.
38. Rebecca Hersman, "Wormhole Escalation in the New Nuclear Age," *Texas National Security Review* 3, no. 3 (Autumn 2020): 96-97.

39. Marcy Fowler, Elin Bergner, and Kristiana Nitisa, "Combating Nuclear Misinformation and Disinformation: Tools, Approaches and the Role of NGOs and International Organizations," Open Nuclear Network (November 2022), 2.
40. Rajeswari Pillai Rajagopalan, "Introduction," in *Future Warfare and Technologies: Issues and Strategies*, Observer Research Foundation, November 24, 2022.
41. Adam Lowther, "The Big and Urgent Task of Revitalizing Nuclear Command, Control, and Communications," *War on the Rocks*, October 4, 2019.
42. Charles Beames, "AI in Space and Its Future Use in Warfare," *Forbes*, December 21, 2022.
43. James Johnson and Eleanor Krabill, "AI, Cyberspace, and Nuclear Weapons," *War on the Rocks*, January 31, 2020.
44. Office of the Secretary of Defense, "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China" (2022), 161-162.
45. Travis Hallen and Michael Spencer, "Hypersonic Air Power," Air Power Development Centre, Royal Australian Air Force, June 25, 2018.
46. Roman C. Lau, "Hypersonic Impacts: Operational Impacts of Hypersonic Weapons and the Change of America's Strategic Situation," Joint Advanced Warfighting School, Joint Forces Staff College, National Defense University (May 2021), 46.
47. Demetri Sevastopulo and Kathrin Hille, "China Tests New Space Capability with Hypersonic Missile," *Financial Times*, October 16, 2021.
48. Jason Sherman, "Hypersonic Weapons Can't Hide from New Eyes in Space," *Scientific American*, January 18, 2022.
49. Senate Armed Services Committee, "Statement of Charles A. Richard, Commander, United States Strategic Command before the Senate Armed Services Committee," March 8, 2022, 25-26.
50. Peter Hayes, "Nuclear Command-and-Control in the Quantum Era," Nautilus Institute, March 29, 2018.
51. Hamish Johnston, "Beijing and Vienna Have a Quantum Conversation," *Physics World*, September 27, 2017.
52. Sarah Jacobs Gamberini and Lawrence Rubin, "Quantum Sensing's Potential Impacts on Strategic Deterrence and Modern Warfare," *Orbis* 65, no. 2 (Spring 2021): 360-362.
53. Durkalec, Gasser, and Shykov, "Multi-Domain Strategic Competition," 12.
54. Erica Lonergan and Keren Yarhi-Milo, "Cyber Signaling and Nuclear Deterrence: Implications for the Ukraine Crisis," *War on the Rocks*, April 21, 2022.
55. David C. Gompert and Phillip C. Saunders, "Sino-American Strategic Restraint in an Age of Vulnerability," *Strategic Forum*, no. 273 (January 2012): 2-8.
56. 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* 4, no. 1 (2021): 124-125.
57. Patrick Morgan, *Deterrence: A Conceptual Analysis* (Beverly Hills, CA: Sage

Publication, 1977), 31-43.
58. James Johnson, "Escalation to Nuclear War in the Digital Age: Risk of Inadvertent Escalation in the Emerging Ecosystem," Modern War Institute, October 13, 2021.
59. Paul A. Goossen, "Cognitive Targeting: A Coercive Air Power Theory for Conventional Escalation Control against Nuclear-Armed Adversaries," School of Advanced Air and Space Studies, Air University (June 2016), 61-96.
60. Edward Geist and Andrew J. Lohn, "How Might Artificial Intelligence Affect the Risk of Nuclear War?" RAND Corporation (2018), 21.
61. Jessica Cox and Heather Williams, "The Unavoidable Technology: How Artificial Intelligence Can Strengthen Nuclear Stability," *Washington Quarterly* 44, no. 1 (2021): 73-77. For a similar view, see also Jennifer Spindel, "Artificial Intelligence and Nuclear Weapons: Bringer of Hope or Harbinger of Doom?" *European Leadership Network*, August 17, 2020.
62. Tess Skyrme, "Quantum Sensors: Advancing Timing, Navigation, Mapping, & Brain Scans," *IDTechEx*, August 2, 2023.
63. Katarzyna Kubiak, "Quantum Technology and Submarine Near-Invulnerability," European Leadership Network (December 2020), 3-9.
64. Geist and Lohn, "How Might Artificial Intelligence Affect the Risk of Nuclear War?" 6.
65. Eva Nour Repussard, "Cyber-Nuclear Nexus: How Uncertainty Threatens Deterrence," Project on Nuclear Issues, Center for Strategic and International Studies, May 10, 2023.
66. Barry Pavel and Christian Trotti, "New Tech Will Erode Nuclear Deterrence. The US Must Adapt," *Defense One*, November 4, 2021.
67. Paul Bracken, "The Hunt for Mobile Missiles: Nuclear Weapons, AI, and the New Arms Race," Foreign Policy Research Institute, September 21, 2020.
68. Dean Wilkening, "Hypersonic Weapons and Strategic Stability," *Survival* 61, no. 5 (October-November 2019): 136-137.
69. Pavel Podvig, "The Myth of Strategic Stability," Bulletin of the Atomic Scientists, October 31, 2012.
70. Matthew Kroenig, "Will Emerging Technology Cause Nuclear War?: Bringing Geopolitics Back In," *Strategic Studies Quarterly* 15, no. 4 (Winter 2021): 59-62.
71. "Quantum Computing and Artificial Intelligence Expected to Revolutionize ISR," Strategic Alternatives Branch, Strategic Plans and Policy, NATO, September 30, 2022.
72. James Johnson, "The AI-Cyber Nexus: Implications for Military Escalation, Deterrence and Strategic Stability," *Journal of Cyber Policy* 4, no. 3 (2019): 448.
73. 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), 4-5.
74. Roger G. Harrison, Deron R. Jackson, and Collins G. Shackelford, "Space Deterrence: The Delicate Balance of Risk," *Space and Defense* 3, no. 1 (Summer 2009): 11-14.
75. Sico van der Meer, "Deterrence of Cyber-Attacks in International Relations: Denial, Retaliation and Signaling," *International Affairs Forum* (Spring 2017), 86.

76. Samantha Ravich and Mark Montgomery, "Harden the Cybersecurity of US Nuclear Complex Now," *C4ISRNet*, October 26, 2022.
77. Kazuto Suzuki, "A Japanese Perspective on Space Deterrence and the Role of the Japan-US Alliance in Sino-US Escalation Management," in *Outer Space; Earthly Escalation? Chinese Perspectives on Space Operations and Escalation*, ed. Nicholas Wright, Department of Defense (August 2018), 45.
78. Matthew R. Crook, "Nuclear Deterrence and the Space and Cyber Domains," Naval Postgraduate School (October 2022), 25.
79. Tim Sweijs and Samuel Zilincik, "The Essence of Cross-Domain Deterrence," in *Deterrence in the 21st Century: Insights from Theory and Practice*, ed. Frans Osinga and Tim Sweijs, Springer (2020), 134.
80. Timothy Georgetti, "U.S. Deterrence in Space: Confusing Constellations for Stars," *Dauntless*, August 28, 2023.
81. Harrison, Jackson, and Shackelford, "Space Deterrence," 22-25.
82. Matthias Schulze, "Cyber Deterrence is Overrated," SWP Comment, no. 34 (August 2019), 3.
83. Crook, "Nuclear Deterrence and the Space and Cyber Domains," 23.
84. Scott D. Sagan and Allen S. Weiner, "The U.S. Says It Can Answer Cyberattacks with Nuclear Weapons. That's Lunacy," *Washington Post*, July 9, 2021.
85. Benjamin Bahney and Anna Péczeli, "The Role of Nuclear-Conventional Intermingling on State Decision-Making and the Risk of Inadvertent Escalation," NSI (November 2021), 7-8.
86. Ankit Panda, "Space-Based Nuclear Command and Control and the 'Non-Nuclear Strategic Attack,'" *Diplomat*, April 8, 2020.
87. James M. Acton, "Cyber Warfare & Inadvertent Escalation," *Daedalus* 149, no. 2 (Spring 2020): 137-141.
88. Chen Dongxiao, "Forewords," in *China-U.S. Cyber-Nuclear C3 Stability*, ed. Ariel E. Levite et al., Carnegie Endowment for International Peace (April 2021), iv.
89. Bill Gertz, "New Strategic Threat Emerging as Weapons Seek to Target Brain Function, Inflict Neurological Damage," *Washington Times*, May 24, 2023.
90. McCreight, "Neuro-Cognitive Warfare."
91. Tosaki, "Emerging Technologies and Nuclear Deterrence Relationship."
92. Geist and Lohn, "How Might Artificial Intelligence Affect the Risk of Nuclear War?" 2-4.
93. Silky Kaur, "One Nuclear-Armed Poseidon Torpedo Could Decimate a Coastal City. Russia Wants 30 of Them," Bulletin of the Atomic Scientists, June 14, 2023.
94. Jill Hruby and M. Nina Miller, "Assessing and Managing the Benefits and Risks of Artificial Intelligence in Nuclear-Weapon Systems," NTI (August 2021), 12-25.
95. Amber Afreen Abid, "Artificial Intelligence in the Nuclear Age," Strategic Vision Institute, October 4, 2023.
96. Nicholas Thompson, "Inside the Apocalyptic Soviet Doomsday Machine," *Wired*, September 21, 2009.
97. Anthony M. Barrett, "False Alarms, True Dangers? Current and Future Risks

of Inadvertent U.S.-Russian Nuclear War," RAND Corporation (2016), 11.
98. "Risks of Artificial Intelligence in Nuclear Command, Control and Communications (NC3): Primer & Policy Options for Risk Mitigation," Future of Life Institute (July 2023), 6-7.
99. Peter Rautenbach, "Keeping Humans in the Loop is not Enough to Make AI Safe for Nuclear Weapons," Bulletin of the Atomic Scientists, February 16, 2023.
100. Alice Saltini, "To Avoid Nuclear Instability, a Moratorium on Integrating AI into Nuclear Decision-Making Is Urgently Needed: The NPT PrepCom Can Serve as a Springboard," European Leadership Network, July 28, 2023.
101. Sweijs and Zilincik, "Cross Domain Deterrence and Hybrid Conflict," 15.
102. Harrison, Jackson, and Shackelford, "Space Deterrence," 23-24.
103. Iain King, "What Do Cognitive Biases Mean for Deterrence?" *Strategy Bridge*, February 12, 2019.
104. Natasha E. Bajema and John Gower, "Nuclear Decision-Making and Risk Reduction in an Era of Technological Complexity," Council on Strategic Risks (December 2022), 96-97.
105. Michael P. Fischerkeller and Richard J. Harknett, "What Is Agreed Competition in Cyberspace?" *Lawfare*, February 19, 2019.
106. Vincent Manzo, "Deterrence and Escalation in Cross-Domain Operations: Where Do Space and Cyberspace Fit," *Strategic Forum*, no. 272 (December 2011): 3-7.
107. Mallory, "New Challenges in Cross-Domain Deterrence," 11.
108. Suzuki Kazuto, "Anzenhosho no kukanteki henyo" [Spatial transformation of security], *Kokusai Mondai* [International Affairs], no. 658 (January/February 2017): 10.
109. Steven Aftergood, "USAF Seeks 'Resilient' Nuclear Command and Control," Federation of American Scientists, April 24, 2019.
110. Office of the Deputy Assistant Secretary of Defense for Nuclear Matters, *Nuclear Matters Handbook 2020*, 21-22.
111. John R. Hoehn, "Nuclear Command, Control, and Communications (NC3) Modernization," *CRS In Focus*, no. IF11697, Congressional Research Service (December 8, 2020)
112. U.S. Air Force, "Battle Management Working to Improve Nuclear Scenario Planning," October 26, 2014.
113. Theresa Hitchens, "Air Force to Kick Off E-4B Replacement Competition in 2021," *Breaking Defense*, February 14, 2020.
114. Courtney Albon, "Northrop Missile-Warning Satellites Pass Early Design Review," *C4ISRNet*, May 24, 2023.
115. Dean Cheng, "Prospects for Extended Deterrence in Space and Cyber: The Case of the PRC," Heritage Foundation, January 21, 2016.
116. James E. Platte, "Defending Forward on the Korean Peninsula: Cyber Deterrence in the U.S.-ROK Alliance," *Cyber Defense Review* 5, no. 1 (Spring 2020): 78-83.
117. Heather Williams et al., "Alternative Nuclear Futures: Capability and Credibility Challenges for U.S. Extended Nuclear Deterrence," Center for Strategic and International Studies (May 2023), 14.
118. Johns Hopkins University & Imperial College London, "Countering Cognitive Warfare: Awareness and Resilience," *NATO Review*, May 20, 2021.
119. Kikuchi Shigeo, "Chugoku no gunjiteki kyoi ni kansuru ninshiki henka to beigun sakusen konseputo no tenkai: Togo zen domein shiki tosei (JADC2) wo 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] 2, no. 2 (March 2022): 42.
120. Michael Klare, "The Military Dangers of AI Are Not Hallucinations," *Foreign Policy in Focus*, July 14, 2023.
121. David Cenciotti, "Let's Have a Look at This Year's NATO Nuclear Strike Exercise in Europe," *Aviationist*, October 28, 2022.
122. Alexander Mattelaer, "Rethinking Nuclear Deterrence: A European Perspective," Centre for Security, Diplomacy and Strategy (May 2022), 5-6.
123. Frank Kuhn, "Making Nuclear Sharing Credible Again: What the F-35A Means for NATO," *War on the Rocks*, September 14, 2023.
124. U.S. Department of Defense, "Department of Defense Announces Pursuit of B61 Gravity Bomb Variant," Immediate Release, October 27, 2023.
125. Aaron Mehta, "US to Introduce New Nuclear Gravity Bomb Design: B61-13," *Breaking Defense*, October 27, 2023.
126. Bates Gill, "Meeting China's Emerging Capabilities: Countering Advances in Cyber, Space, and Autonomous Systems," National Bureau of Asian Research, December 15, 2022.
127. Victoria Samson and Brian Weeden, "Enhancing Space Security: Time for Legally Binding Measures," Arms Control Association (December 2020).
128. Gabriel Molini, "The Evolving Cyber-Based Threat: The Need for International Regulations to Avoid 'Accidental' Conflicts," Center for Arms Control and Non-Proliferation, September 12, 2023.
129. Victoria Samson, "Breaking the Impasse over Security in Space," Arms Control Association (September 2022).
130. Mary Chesnut, "The 21st Century Space Race Is Here," *National Interest*, October 17, 2019.
131. Ibid.
132. United Nations Institute for Disarmament Research, "Restoring Confidence across Today's Nuclear Divides: Symposium Report," UNIDIR (2021), 5.
133. Daryl G. Kimball, "Space Security Working Group Meets," Arms Control Association (June 2022).
134. Andrew Futter, "What Does Cyber Arms Control Look Like? Four Principles for Managing Cyber Risk," European Leadership Network (June 2020).
135. Heather M. Williams and Nicholas Smith Adamopoulos, "Arms Control after Ukraine: Integrated Arms Control and Deterring Two Peer Competitors," Center for Strategic and International Studies (December 2022), 8.
136. "B61-12 Nuclear Bomb," Airforce-technology.com website.
137. "Neuroweapons: Breakthroughs in Science Change Future Weapons," *Vision of*

Humanity, n.d.
138. Lauren Kahn, "Mending the 'Broken Arrow': Confidence Building Measures at the AI-Nuclear Nexus," *War on the Rocks*, November 4, 2022.
139. Zachary Kallenborn, "AI Risks to Nuclear Deterrence Are Real," *War on the Rocks*, October 10, 2019.
140. Spenser A. Warren, "Avangard and Transatlantic Security," Center for Strategic and International Studies, September 23, 2020.
141. UNIDIR, "Restoring Confidence across Today's Nuclear Divides," 5.
142. "Russia Shows Willingness to Include New Nuke, Hypersonic Weapon in Arms Control Pact," *Defense News*, April 18, 2020.
143. Hayes, "Nuclear Command-and-Control in the Quantum Era."
144. Sandra Erwin, "Mattis to Decide Future of Nuclear Command, Control and Communications," *Space News*, April 11, 2018.