SIPRI Research Policy Paper
January 2026

ADDRESSING MULTIDOMAIN NUCLEAR ESCALATION RISK

WILFRED WAN*

SUMMARY

● **Contemporary warfare is characterized by military operations that encompass multiple arenas—from air, land and sea to the increasingly prominent cyber, outer space and information domains—and feature the convergence of advanced technological capabilities. New vectors of vulnerability stemming from this and from increasing interactions between nuclear and non-nuclear capabilities raise the spectre of escalation and introduce new potential pathways for nuclear weapon use.**

These new risks have not been thoroughly explored in national policies or multilateral forums. Effectively addressing multidomain escalation risk requires that nuclear-armed states revisit the concept of 'strategic stability' and systematically map multidomain escalation scenarios while engaging non-nuclear-armed states and other stakeholders. The toolkit for avoiding and managing crisis also needs to be updated to reflect multidomain risk scenarios. These and other pragmatic steps can help prevent escalation pathways from coming into fruition. A longer-term approach is required to reverse both arms racing trends and current thinking regarding strategic capabilities.

In June 2025 Ukraine launched an unprecedented attack deep within the Russian Federation. The covert operation 'Spider Web' involved the use of 117 uncrewed aerial vehicles (UAVs) to target airfields across the country.[1] Trained through artificial intelligence (AI) and reportedly costing at most a few thousand dollars each, the UAVs avoided potential Russian countermeasures and caused damage or destruction at an estimated cost of US$7 billion.[2] Ukraine's target appeared to be Russian long-range aircraft that have delivered the cruise missiles used in the war. Yet an estimated 10–13 of the strategic bombers disabled in the attack were also capable of carrying nuclear weapons; Russian nuclear forces were effectively undermined.[3]

Operation Spider Web marked a notable demonstration of the use of emerging technologies across multiple operational domains in the Russia–Ukraine War; the first was in the early hours of the full-scale invasion on 22 February 2022, with a cyberattack on the Viasat network, probably targeted at the Ukrainian military's satellite communications.[4] Overall, the ongoing war—alongside the May 2025 India–Pakistan conflict and Israel's June 2025 military operations in Iran—exhibits the rapidly evolving battlefield that is marked by convergence of technologies and the regular presence of multidomain operations that can cross from the historically predominant air, land and sea domains to the increasingly prominent cyber, outer space and information domains.[5]

As in the case of Spider Web, the spillover effects of these operations can have an impact on both conventional and nuclear capabilities. Further conventional–nuclear entanglement appears inevitable in the current landscape.[6] In such circumstances, where 'traditional firebreaks between

[1] Collett-White, M., Kumar Dutta, P. and Zafra, M., 'How Ukraine pulled off an audacious attack deep inside Russia', Reuters, 4 June 2025; and 'Significance and implications of Ukraine's Operation Spiderweb', Trends Research & Advisory, 3 June 2025.

[2] Kirichenko, D., 'Ukraine's cheap robot drones extract a heavy price from Russia', The Interpreter, Lowey Institute, 5 June 2025.

[3] Mihayloff, A., 'Ukraine attacks part of Russia's nuclear triad. Russia may strike nuclear blow in response', Pravda.ru, 2 June 2025.

[4] Saalman, L., Su, F. and Dovgal, L., 'Cyber crossover and its escalatory risks for Europe', SIPRI Insights on Peace and Security no. 2023/09, Sep. 2023.

[5] Riboua, Z., 'How Israel's Operation Rising Lion dismantled Iran from within: A case study in the art of deception', Hudson Institute, 13 June 2025; Akhtar, R., 'Escalation gone meta: Strategic lessons from the 2025 India–Pakistan crisis', Belfer Center for Science and International Affairs, 14 May 2025; and North Atlantic Treaty Organization (NATO), Allied Command Transformation, 'Multi-domain operations in NATO—Explained', 5 Oct 2023.

[6] Acton, J. M., 'Escalation through entanglement: How the vulnerability of command-and-control systems raises the risks of an inadvertent nuclear war', *International Security*, vol. 43, no. 1 (summer 2018).

* The author would like to express his sincere gratitude to the Global Challenges Foundation for supporting this research.

conventional and nuclear . . . systems erode', the notion of strategic stability—conceived narrowly here as the absence of incentives for nuclear attacks (crisis stability) and of incentives for building up nuclear forces (arms race stability)—appears increasingly elusive.[7] Escalation pathways, including to nuclear use, are becoming more complex, unpredictable and numerous.

This research policy paper outlines the nature of multidomain escalation risk in a contemporary strategic context marked by shifts in global power dynamics. It first considers how the policies of nuclear-armed states both acknowledge and perpetuate emerging escalation pathways. The paper then examines how multidomain operations can contribute to nuclear escalation risk by upending strategic relations and throwing into question common understandings of the nuclear threshold. Having presented some thoughts on an effective governance approach to address multidomain escalation risk, including with the identification of near-term opportunities, the paper concludes by outlining a longer-term holistic approach to reducing nuclear risk.

I. Presumptions of strategic instability

Following operation Spider Web, some Russian experts suggested the possibility of a nuclear response; some military bloggers explicitly called for it.[8] While there was no such clamour at the official level, the possibility for multidomain escalation that breaches the nuclear threshold has been recognized for some time. During the cold war, there was a particular concern about inadvertent escalation pathways, in which conventional operations would raise the target's concerns about an imminent nuclear decapitation attack, fuelling a 'use it or lose it' scenario.[9] Yet today there are 'new and more complex pathways' to escalation, both deliberate and inadvertent, linked to technological developments.[10] This is also because, in the newer domains, there is no 'collective experience, common understandings, and established norms of behavior', while there is an increasing 'interplay between nuclear and non-nuclear strategic capabilities'.[11] Yet these new risk possibilities have not been thoroughly explored in national policies, with only oblique references to 'unpredictable risks and challenges' and an acknowledgement of the 'growing risk of uncontrolled escalation'.[12]

There thus now exists a more complex strategic environment and what could be considered a new 'strategic equation', in which technological

[7] Hersman, R., 'Wormhole escalation in the new nuclear age', *Texas National Security Review*, vol. 3, no. 3 (autumn 2020), p. 92. The definition of strategic stability is taken from Acton, J. M., 'Reclaiming strategic stability', eds E. A. Colby and M. S. Gerson, *Strategic Stability: Contending Interpretations* (US Army War College, Strategic Studies Institute: Carlisle, PA, Feb. 2013), p. 117.

[8] Mihayloff (note 3); and 'Caught in the Spider's Web: Military bloggers revealed gaps in Russia's military and information defense', German Marshall Fund, 26 June 2025.

[9] Posen, B. R., *Inadvertent Escalation: Conventional War and Nuclear Risks* (Cornell University Press: Ithaca, NY, 1991), p. 28.

[10] British Ministry of Defence (MOD), *Strategic Defence Review—Making Britain Safer: Secure at Home, Strong Aboard* (MOD: London, 2025), p. 27.

[11] US Department of Defense (DOD), '2022 Nuclear Posture Review', *2022 National Defense Strategy of the United States of America* (DOD: Washington, DC, Oct. 2022), p. 6.

[12] Chinese State Council, [China's national security in the new era], White paper (State Council Information Office: Beijing, May 2025), chapter 2 (in Chinese), unofficial translation Foreign Languages Press, [26 June 2025], p. 6; and French General Secretariat for Defence and National Security (SGDSN), *National Strategic Review 2025* (SGDSN: Paris, 2025), p. 20.

developments are contributing to a wider array of relevant capabilities—including offensive cyber capabilities and advanced conventional precision-strike capabilities—that can have an impact on strategic stability, including by putting nuclear forces at risk. Related to this is the greater number of actors—including non-nuclear armed states—that possess and deploy these different capabilities across domains. Given these realities, it is especially concerning that some states are concurrently widening the range of circumstances in which they would consider using their nuclear weapons. As a means of deterring the North Atlantic Treaty Organization (NATO) and the West in general, in 2024 Russia altered its principles of nuclear deterrence to include the use of nuclear weapons against aggression 'by any non-nuclear state' with support of a nuclear-armed state; and, in response to perceived aggression from South Korea and the United States, in 2022 North Korea adopted a pre-emptive doctrine that includes attack against a non-nuclear-armed state working 'in collusion' with a nuclear-armed state.[13]

Beyond these explicit changes, strategic ambiguity has long been a feature of existing doctrines and postures. For instance, US nuclear forces aim to 'deter all forms of strategic attack' and Pakistan's forces aim to counter the 'full-spectrum' of potential threats within the 'precincts of credible minimum nuclear deterrence'.[14] The issue is that those forms of threat and attack are expanding; and, consequently, so is the range of ambiguity. These shifts are also having an impact on force postures. For instance, France has noted that 'changes in the strategic environment call for ensuring the relevance of the capability choices'.[15] This suggests potential changes to the future composition of its nuclear forces, which have already received significant investment (e.g. the announcement of the establishment of a new nuclear base).[16]

II. Escalation variables

Just as nuclear-armed states predict increased strategic instability, they may be fulfilling those prophecies, including by integrating non-nuclear strategic operations and the activities of non-nuclear armed states into their doctrines. In addition, expanded strategic ambiguity can open up more unpredictable escalation pathways and lead to longer-term arms racing dynamics. Even below the nuclear threshold, operations in the newer domains can have generally destabilizing effects—for instance, in the case of non-kinetic operations (featuring activities that do not have physical effects, including lasers, electronic interference or cyber operations), what acts could be seen as reaching the threshold of 'use of force' or 'armed attack' under international law? Multidomain operations—through their increased commingling and entanglement of conventional and nuclear systems, their blurring of offensive and defensive intentions, and their complicating of deterrence practices and signalling—also contribute to greater operational ambiguity.

[13] 'Fundamentals of state policy of the Russian Federation on nuclear deterrence', approved by Russian Presidential Order no. 991, 19 Nov. 2024, para. 11; and Korean Central News Agency (KCNA), 'Law on DPRK's policy on nuclear forces promulgated', KCNA Watch, 9 Sep. 2022.

[14] US Department of Defense (note 11), p. 7; and Pakistani National Security Division, 'National security policy of Pakistan 2022–2026', [2022], p. 3.

[15] French General Secretariat for Defence and National Security (note 12), p. 24.

[16] Kristensen, H. M. et al., 'French nuclear weapons, 2025', *Bulletin of the Atomic Scientists*, vol. 81, no. 4 (July 2025).

Pushing boundaries

These complex dynamics have been evident in the Russia–Ukraine War.[17] The damage to dual-capable bombers in operation Spider Web, for instance, left open the question of whether Russia might conclude that there was a degree of Western involvement or whether Ukraine's intent was, indeed, to damage Russia's nuclear forces—and whether and how Russia may respond, depending on its answers to those questions. While Ukraine reportedly did not inform the USA or others prior to its operation, that only underscores how third parties (and non-nuclear-armed states) can affect relations between nuclear-armed states.[18] The Russia–Ukraine War has also included a spate of incidents—in addition to the Viasat cyberattack—involving cyber operations that have had an impact on satellite infrastructure and triggered false missile alarms. The essential role that space systems play in nuclear deterrence could mean that such incidents could 'elicit conventional or even nuclear retaliation' if they involve nuclear-armed states on both sides.[19]

Meanwhile, in South Asia, following the terrorist attacks near Pahalgam in Indian-controlled Kashmir in April 2025, AI-enabled disinformation could easily have spiralled into an extended conflict, with direct nuclear confrontation between India and Pakistan a possibility. In the aftermath of the attacks undertaken by India against alleged terrorist bases in Pakistan, there was a 'carnival of sensationalism', with artificially generated content driving false narratives of successes against strategic targets and captured territories broadcast on mainstream media outlets on both sides.[20] The chief of India's Defence Staff observed that the Indian military devoted substantial resources to countering these as part of the 'non-contact and multi-domain' conflict that 'exemplifies the future of war'.[21] There is a risk that similar AI-enabled disinformation efforts could more successfully obfuscate battlefield realities and upend the strategic calculus of the nuclear-armed states in such crises in the future.

Challenging assumptions

Something that is especially concerning in the context of multidomain operations is that, for many scenarios, there is little or no precedent. For example, a state might consider undertaking unnotified manoeuvres involving a dual-use space asset (i.e. one that could serve both conventional and nuclear missions) as a target. However, the lack of a baseline of expectation or a common risk framework means that the attacking state and the targeted state could make different assessments of how escalatory the operation is.[22] This can create an escalatory spiral. Even different ministries and divisions

[17] van Hooft, P., Ellison, D. and Swijs, T., *Pathways to Disaster: Russia's War against Ukraine and the Risks of Inadvertent Nuclear Escalation* (The Hague Centre for Strategic Studies: The Hague, May 2023).

[18] Dahlgren, M. and MacKenzie, L., 'Ukraine's drone swarms are destroying Russian nuclear bombers. What happens now?', Center for Strategic and International Studies (CSIS), 4 June 2025.

[19] Saalman, L., Savaleva Dovgal, L. and Su, F., 'Mapping cyber-related missile and satellite incidents and confidence-building measures', SIPRI Insights on Peace and Security no. 2023/10, Nov. 2023, p. 1.

[20] Gupta, N., 'When India and Pakistan went to war—online', The Diplomat, 22 May 2025.

[21] Pandit, R., 'Spent 15% of time nixing fake news during Op Sindoor: CDS Anil Chauhan', *Times of India*, 1 June 2025.

[22] Raju, N., 'Parameters to assess escalation risks in space', SIPRI Research Policy Paper, Feb. 2025.

within a state, given their different functions, interests and cultures, might make different assessments. Some argue that the uniquely 'multifaceted nature of national interests' in outer space—linked to the overlay of military, economic, political and other priorities in the domain—creates an inherently complex policymaking discourse.[23] The lack of coordinated response can also contribute to a destabilizing environment.

Meanwhile, the more frequent, pervasive and strategic use of cyber operations arguably demands a 'rethink of years-old assumptions', including of mutual understandings of whether such operations constitute use of force.[24] While small, seemingly discrete incidents may not be taken as crossing the use-of-force threshold, this assessment might change if they were to build cumulatively over time, creating escalatory effects. This is especially likely if there are kinetic effects or impacts on critical infrastructure—as happened in 2010 with the Stuxnet worm, which damaged Iranian nuclear centrifuges, or with ongoing disruptions of essential civilian services linked to power grids in Ukraine.[25] The likelihood of a change of assessment may be affected by expanding nuclear alliances and strategic partnerships; a related dynamic is the potential for conflicting perceptions of risk and threat even among alliance partners, which can complicate external signalling or inspire inconsistent responses.[26]

Overall, assumed national competencies in escalation control or escalation management on all sides can drive complacency and inhibit efforts to update approaches for multidomain operations, including responses to them. This also has the potential to embolden more aggressive behaviour. 'Learning by doing', as some characterize US escalation-management strategy in response to Russian nuclear signalling in Ukraine, is likely to feature with multidomain operations given the preponderance of considerations associated with new capabilities and domains and the lack of precedent.[27] But this strategy could result in misperception, miscalculation or misunderstanding that will drive escalation, including potentially past the nuclear threshold.

III. Multidomain de-escalation

Governance approaches

While there has been modest movement in multilateral forums to address the destabilizing impacts of emerging technologies and domains, these discussions have centred so far on general principles—on the military use of AI or on the prevention of an arms race in outer space (PAROS), for instance. The likelihood of restraints that extend to new capabilities or to newer domains appears low—these are likely to be eclipsed from two directions.

[23] Wu, X., 'The interplay of domestic policy and international space security', eds S. M. Pekkanen and P. J. Blount, *The Oxford Handbook of Space Security* (Oxford University Press: Oxford, 2024), p. 147.

[24] Sherman, J., *Confronting Russia's Cyber Power: Reassessing Assumptions, Sizing Up the Threat, and Building a Proactive Response* (Atlantic Council: Washington, DC, May 2025), p. 2.

[25] Kile, S. N., 'Nuclear arms control and non-proliferation', *SIPRI Yearbook 2011: Armaments, Disarmament and International Security* (Oxford University Press: Oxford, 2011), p. 384; and Saalman et al. (note 4).

[26] Raju, N. and Grego, L., *The Space–Nuclear Nexus in European Security* (SIPRI: Stockholm, June 2025).

[27] Stein, J. G., 'Escalation management in Ukraine: "Learning by doing" in response to the "threat that leaves something to chance"', *Texas National Security Review*, vol 6, no. 3 (summer 2023).

From nuclear-armed states comes the desire to acquire strategic advantage in a competitive security environment. Meanwhile, from non-nuclear armed states comes the desire to fulfil their technological ambitions, including as means to overcome asymmetries in capabilities. Such dynamics are exacerbated by the limited direct dialogue among nuclear-armed states across all settings. By facilitating exchange on developing capabilities and multidomain operations, that dialogue might contribute to a degree of strategic predictability and the development of the common risk framework that is critical to ensuring that nuclear-use thresholds hold.

Of even greater concern is the frayed status of the risk-reduction and de-escalation toolkit developed from the cold war period and sustained following the dissolution of the Soviet Union. This has been yet another victim of deteriorated relations between Russia and the West. While mechanisms such as the Vienna Document 2011 and the 1992 Open Skies Treaty focused on historically predominant domains and capabilities, their collapse or deterioration means that there is no longer a framework for information exchange, military transparency and consultation in which new strategic capabilities could be considered.[28] Meanwhile, intensifying strategic competition between China and the United States raises obstacles to the development of a comparable framework in that relationship.[29] There is, nonetheless, widespread political support for reducing nuclear risk in the abstract, including as seen in recent review cycles of the 1968 Treaty on the Non-Proliferation of Nuclear Weapons (NPT).[30] However, demonstrable action on any such steps remains largely absent. Multidomain escalation risk is a legitimate concern in this context: strategic meaning is being infused into regional conflict, while states are looking with suspicion at the activities of their adversaries' allies and partners—with inadvertent nuclear use a potential outcome.

Nearer-term opportunities

An all-encompassing governance approach to effectively addressing multidomain escalation risk requires the following elements as a start. While the near-term process requires leadership by nuclear-armed states in particular, the outlined recommendations can help not only reorient but also expand the conversation to non-nuclear states and other stakeholders—enabling a longer-term approach that reflects the more complex environment.

Revisit 'strategic stability'

Nuclear-armed states should revisit and clarify notions of strategic stability given technological developments. In particular, they should elaborate

[28] Vienna Document 2011 on Confidence- and Security-Building Measures, issued by Organization for Security and Co-operation in Europe (OSCE) Forum for Security Co-operation Decision no. 14/11, 30 Nov. 2011, entered into force 1 Dec. 2011; and Treaty on Open Skies, opened for signature 24 Mar. 1992, entered into force 1 Jan. 2002, *Canada Treaty Series* (2002), no. 3.

[29] Wu, R., 'Why isn't China interested in nuclear risk reduction?', Lawfare, 7 Sep. 2025.

[30] 2020 NPT Review Conference, 'A nuclear risk reduction package', Working paper submitted by the Stockholm Initiative, 2020 Review Conference of the Parties to the Treaty on the Non-Proliferation of Nuclear Weapons, NPT/CONF.2020/WP.9/Rev.1, 12 Aug. 2022; and Treaty on the Non-Proliferation of Nuclear Weapons (Non-Proliferation Treaty, NPT), opened for signature 1 July 1968, entered into force 5 Mar. 1970, IAEA INFCIRC/140, 22 Apr. 1970.

what they perceive as challenges to that stability. While these states acknowledge the presence of multidomain risk in their nuclear doctrines and security strategies, they too often characterize this risk as unpredictable or uncontrollable. Yet this detachment can allow states to evade responsibility and avoid more critical examination of their national doctrines and investments.

In this strategic context, a pragmatic way forward may be for states to explore the conceptions of strategic stability within their national security apparatuses, across their ministries, with the private sector and in consultation with their allies. Committing to proactively identify necessary steps to maintain strategic stability in the face of multidomain operations, including by re-evaluating national approaches to escalation control, constitutes a necessary first step to addressing associated risk. Ultimately, however, reducing nuclear risk will require a more systematic approach to preventing multidomain escalation pathways, including through efforts at bilateral, regional and, especially, multilateral and global levels, while engaging the wider group of stakeholders linked to relevant developments across domains.

Map multidomain escalation scenarios

States—both nuclear-armed and non-nuclear armed—should undertake work to map multidomain escalation scenarios, with a view towards the development of more common risk understandings and frameworks. This may include exchanges on the roles and strategic valuations of particular capabilities and systems, on activities and behaviours they find especially escalatory, and on how deterrence concepts may apply in the cyber and outer space domains (and how these interact with traditional domains of warfare), to the extent possible. This mapping can also engage civil society and members of the expert community.

These exchanges would necessitate inclusion of multidomain escalation risk in the mainstream conversation—including initially by simply raising awareness of this risk—across relevant governance forums. This could include, for instance, the ongoing United Nations open-ended working groups (OEWGs) on PAROS or information and communications technology (ICT).[31] Dialogue must also extend beyond nuclear command, control and communications (NC3), often the focal point of technological discussions, to include the broader environment in which nuclear decisions may take place.[32]

More detailed dialogue between states—for instance, on escalation thresholds and on legitimate, proportionate responses—can begin with like-minded states, including but not limited to alliance settings.[33] Through wargaming and joint military exercises, this can strengthen deterrence signalling to adversaries, and thereby reduce strategic ambiguity and the possibility of miscalculation, misperception and misunderstanding. State-led initiatives

[31] On the PAROS and ICT processes in the UN see e.g. Raju, N., 'Space security governance', *SIPRI Yearbook 2025: Armaments, Disarmament and International Security* (Oxford University Press: Oxford, 2025), pp. 371–77; and Pytlak, A., 'Cyber and digital threats', *SIPRI Yearbook 2025*, pp. 359–61.

[32] Su, F. et al., *Pragmatic Approaches to Governance at the Artificial Intelligence–Nuclear Nexus* (SIPRI: Stockholm, Oct. 2025).

[33] Raju, N., 'Strengthening NATO's deterrence and defense posture in outer space', eds N. Fasola et al., *Space: Exploring NATO's Final Frontier* (NATO Allied Command Transformation: Norfolk, VA, 2024).

linked to UN processes can provide another conduit for exchange. As geopolitical conditions improve, these established strategic valuations can eventually become the basis of exchange and negotiation beyond the like-minded, towards multilateral regulatory frameworks.

Update crisis-prevention and -management mechanisms

States should update existing mechanisms—both bilateral and broader—for crisis prevention and management to account for multidomain scenarios. In recent years, for instance, some states that have signed incidents at sea (INCSEA) agreements have updated these to specify acceptable distances between vessels, account for new systems (including the use of lasers) and establish new procedures—as Norway and Russia did in 2021 to include deep-sea remotely operated vehicles and to expand the zone of coverage.[34]

In the context of the cross-cutting effects of emerging technologies and domains, there should be a concerted effort to revisit arrangements across the board, including the Russia–USA Agreement on the Prevention of Dangerous Military Activities (DMA) or, in the Asia-Pacific, the voluntary Code of Unplanned Encounters at Sea (CUES) and Guidelines for Air Military Encounters (GAME).[35] Building also on the initial discussions between Russia and the USA in 2021 on declaring NC3 off limits to cyber operations, this may entail rethinking what it means to engage in risky or provocative behaviour, especially behaviour for which there is no precedent or which involves non-kinetic operations.[36] This would reflect a broader behavioural approach to arms control, which could provide a constructive basis to advance discussions.[37]

Put multidomain risk on the agenda in regional and subregional forums

States should acknowledge—and advance concrete discussion on—multi-domain risk in regional and subregional forums, since these can be especially conducive to strengthening conflict-avoidance and -management frameworks. In the past decade, for instance, states have sought to establish points of contact for cyber incidents in regional security frameworks and have built capacities in maritime awareness in locales as dispersed as the Baltic Sea and the South China Sea. This has involved, among other activities, convening workshops, exchanging information and engaging in tabletop exercises.

A more holistic perspective on such efforts—one that bridges domains—within a region can acknowledge the interactive and cumulative effects of these incidents on escalation and security thinking. This can constitute a first step to discussing multidomain issues at the global level. In a similar vein, linking conversations about regional and subregional security environments

[34] 'Norway and Russia sign updated agreement on Security at Sea', *High North News*, 21 Dec. 2021; and O'Dwyer, G., 'Norway and Russia sharpen transparency pact on warship, aircraft moves', *Defense News*, 20 Aug. 2021.

[35] Soviet–United States Agreement on the Prevention of Dangerous Military Activities, signed 12 June 1989, entered into force 1 Jan. 1990, *United Nations Treaty Series*, vol. 1566 (1990); Code for Unplanned Encounters at Sea, version 1.0, Western Pacific Naval Symposium, 22 Apr. 2014; and Guidelines for Air Military Encounters, adopted by the Association of Southeast Asian Nations (ASEAN) Defence Ministers' Meeting, 19 Oct. 2018.

[36] Sanger, D. E., 'Once, superpower summits were about nukes. Now, it's cyberweapons', *New York Times*, 15 June 2021.

[37] Kühn, U. and Williams, H., 'Behavioral arms control and East Asia', *Journal for Peace and Nuclear Disarmament*, vol. 7, no. 1 (May 2024).

to those about strategic relations involving nuclear-armed and nuclear-allied states can help increase strategic awareness and mutual understanding. This in turn may lessen risky behaviours and deployments, including by non-nuclear armed states, and may even slow arms racing dynamics, thus contributing to longer-term regional and strategic stability.

Take a forward-looking approach to strategic technologies in global governance

States need to take a more forward-looking approach to strategic technologies in global governance. This should include a more regularized engagement with the private sector and industry, given their leading role in technological developments that form the foundation for multidomain operations.

This would require creating platforms that incorporate the private sector, as seen in the Responsible AI in the Military Domain (REAIM) summits and related activities. This also requires that states discuss, including in UN forums, the governance of these actors and their activities under international law. The need for this has been underlined by the example of SpaceX in the Russia–Ukraine War, in which the company has had a direct impact on military operations.

It is also essential that global governance structures aim to more systematically track relevant developments in science and technology that can upend strategic stability in the future. The NPT—the centrepiece of global nuclear governance—is lagging in this respect despite shifts in national doctrines and force postures linked to those technologies; other arms control regimes can offer potential modalities to take these evaluations forward. Examples include the Scientific Advisory Board (SAB) of the 2017 Treaty on the Prohibition of Nuclear Weapons; the Centre for Chemistry and Technology and the SAB of the Organisation for the Prohibition of Chemical Weapons (OPCW) under the 1992 Chemical Weapons Convention; and discussions on a science and technology review mechanism in the 1972 Biological Weapons Convention.[38] Regularized engagement between chairs of different UN processes and across structures, including the Office for Outer Space Affairs (UNOOSA) and the Office for Disarmament Affairs (UNODA), as convened by the UN secretary-general, could further enable a more forward-looking approach to strategic technologies.

IV. Towards a holistic approach

A number of processes under the auspices of the UN, including the ongoing OEWG on PAROS and the upcoming 2026 NPT Review Conference, present pivotal opportunities for states to begin in earnest the effort to address multidomain escalation risk. Focusing on inadvertent escalation pathways could be an entry point into the topic. But stakeholders will eventually

[38] See e.g. Treaty on the Prohibition of Nuclear Weapons, Meeting of States Parties, 'Update to the 2023 report of the Scientific Advisory Group on the status and developments regarding nuclear weapons, nuclear weapon risks, the humanitarian consequences of nuclear weapons, nuclear disarmament and related issues', Working paper submitted by the Scientific Advisory Group, TPNW/MSP/2025/WP.5, 21 Feb. 2025; Anthony, I., 'The Centre for Chemistry and Technology and the future of the OPCW', SIPRI Research Policy Paper, Mar. 2024; and Revill, J., Anand, A. and Persi Paoli, G., *Exploring Science and Technology Review Mechanisms Under the Biological Weapons Convention* (UN Institute for Disarmament Research: Geneva, 2021).

need to broach deliberate escalation, given the widening scope of strategic capabilities and more expansive notions of nuclear deterrence linked to multidomain operations.

The first steps include intensifying discussions of multidomain operations and of interactions between AI, cyber, outer space, advanced conventional and nuclear capabilities. There must also be an initial dialogue on the concrete ways in which these have an impact on escalation pathways. These discussions may require states to parse their own nuclear doctrines and security strategies and to make a commitment to exchanging views on updated deterrence concepts. It may also require existing de-escalation mechanisms to be revisited and reviewed.

It will also be necessary to de-silo governance across capabilities and agencies and to also involve non-nuclear armed states as well as the private sector. This would acknowledge the potential catastrophic nuclear consequences of escalation and allow the development of a broader strategic value structure that can reduce the likelihood of misperception, miscalculation and misunderstanding. It would also inspire concrete steps to prevent escalation from breaching the nuclear threshold. Ultimately, addressing multidomain nuclear escalation risk in this manner could reverse the long-term destabilizing trends linked to emerging technologies and domains and lead to the revitalization of arms control and disarmament efforts.

Abbreviations

AI	Artificial intelligence
ICT	Information and communications technology
NC3	Nuclear command, control and communications
NPT	Treaty on the Non-Proliferation of Nuclear Weapons (Non-Proliferation Treaty)
OEWG	Open-ended working group
PAROS	Prevention of an arms race in outer space
SAB	Scientific Advisory Board
UAV	Uncrewed aerial vehicle
UN	United Nations

SIPRI RESEARCH POLICY PAPER

ADDRESSING MULTIDOMAIN NUCLEAR ESCALATION RISK

WILFRED WAN

CONTENTS

ABOUT THE AUTHOR

Dr Wilfred Wan is Director of the SIPRI Weapons of Mass Destruction Programme, where his research focuses on nuclear weapon risk reduction, nuclear disarmament verification, and other issues related to arms control and disarmament. Prior to joining SIPRI, Wan worked at the United Nations Institute for Disarmament Research, the UN University Centre for Policy Research, Hitotsubashi University and Harvard Kennedy School's Belfer Center for Science and International Affairs. His recent publications include *Pragmatic Approaches to Governance at the Artificial Intelligence–Nuclear Nexus* (Oct. 2025, co-author).

STOCKHOLM INTERNATIONAL PEACE RESEARCH INSTITUTE
Signalistgatan 9
SE-169 72 Solna, Sweden
Telephone: +46 8 655 97 00
Email: sipri@sipri.org
Internet: www.sipri.org

DOI: https://doi.org/10.55163/XMPJ2147