YOUNG LEADERS PROGRAM

REINFORCING U.S. EXTENDED NUCLEAR DETERRENCE IN THE INDO-PACIFIC

BY AARON CHAN

Aaron Chan *is the Managing Director of Young Professionals in Foreign Policy and specializes in transnational climate and security policy, the Indo-Pacific, and international youth diplomacy. He has worked on US national security and foreign policy in Congress, think tanks, and across federal agencies.*

Photo: Trucks transport what appear to be North Korea's Musudan intermediate-range ballistic missiles at a military parade in Pyongyang on October 10, 2010. Source: CNN

The global security environment is shifting rapidly, and with it, the challenges facing the United States and its allies. Increasing alignment between nations like China, Russia, and North Korea is testing the foundations of U.S. extended deterrence, particularly in the Indo-Pacific. As the geopolitical landscape becomes more complex, the importance of denying adversaries the opportunity to exploit vulnerabilities is more vital than ever.

In the spring of 2025, the Center for Global Security Research (CGSR) at Lawrence Livermore National Laboratory hosted a strategy colloquium focused on these very issues. The event brought together a diverse group of national security thinkers to discuss how to strengthen U.S. deterrence posture in the Indo-Pacific. This article draws on those discussions. It's written to provide insights for defense and strategic planners, and it represents the author's viewpoints and reflections of the workshop.

Understanding the Multipolar Challenge

The Indo-Pacific is no longer defined by one or two threats—it's a region shaped by a convergence of actors, interests, and strategies. The growing coordination between China and Russia, combined with the continued provocations from North Korea and the destabilizing behavior of Iran, presents a complex web of challenges. These countries are learning to exploit weak points in the current deterrence system, not just through direct military action but also through economic coercion, cyber tactics, and ambiguous or "gray zone" activities that test the limits of U.S. and allied responses. For instance, Russian cyber-attacks like the infamous NotPetya cyber-attack caused significant economic loss. However, because gray zone actions fall below conventional thresholds of retaliation and don't fit cleanly into existing laws or doctrines, they make it difficult for the US and its partners to coordinate a clear and unified response. Looking back at the NotPetya cyber-attack, even after the U.S. and U.K. formally attributed the attack to the Russian GRU, there was no direct reprisal or legal consequence. Was the attack an act of war, cybercrime, or economic sabotage? In this way, gray zone activities push the limits of international systems while skirting the limits of reprisal.

One of the key takeaways from the CGSR seminar was the increasing possibility that these adversaries may engage in opportunistic aggression—timed and targeted to catch the U.S. or its allies off guard. Whether acting in concert or independently, their aim is to push boundaries, erode trust between partners, and challenge the credibility of U.S. security guarantees.

Complicating matters further, adversaries are developing sophisticated capabilities across a range of domains—not just nuclear and conventional forces, but also cyber, space, and information warfare. These tools allow them to pressure the U.S. and its

allies in ways that don't always trigger a traditional military response. The implication is clear: future deterrence must be multidimensional, integrating both old and new technologies, and combining diplomatic, military, and strategic communications in smarter ways.

The Debate Around Secondary Decision Centers

One of the more thought-provoking concepts discussed at the colloquium was the idea of "secondary decision centers." Simply put, these refer to U.S. allies developing more independent roles in deterrence—whether by acquiring their own nuclear capabilities or by gaining greater autonomy in how they manage regional threats.

There's a case to be made for this. Supporters argue that empowering regional allies—especially those on the front lines—could strengthen deterrence by making it harder for adversaries to predict or plan aggression. The presence of multiple deterrent actors might create more uncertainty for would-be aggressors and give the broader alliance network more strategic depth.

But the idea isn't without risks. Independent deterrent capabilities could lead to strategic confusion, especially if national interests start to diverge or if coordination falters. The chance for miscommunication, unintentional escalation, or overlapping authorities could increase. There's also a risk that wider proliferation of nuclear weapons, even among allies, could weaken global nonproliferation norms and add fuel to already tense regional dynamics.

The conversation also raised bigger questions about how alliances function in today's world. Can partners with independent deterrent roles still speak with one voice? Can they coordinate responses quickly and clearly in a crisis? These are not just technical

questions—they go to the heart of how trust and leadership work in multilateral security arrangements.

What It Means for U.S. Deterrence Strategy

The growing interest among allies in building up their own capabilities reflects a larger concern: some countries no longer see U.S. guarantees as absolute. Whether this is a matter of perception or reality, it's driving moves toward greater self-reliance in defense. For Washington, this shift poses a delicate challenge. Should the U.S. support these efforts and risk strategic fragmentation, or try to maintain a more centralized command structure that some allies may see as limiting?

Finding the right balance will be crucial. Delegating more authority to allies can strengthen regional deterrence and lighten the load on U.S. forces—but only if there are strong mechanisms in place for coordination, communication, and crisis management. This means updating shared plans, running more joint exercises, and aligning strategic goals as closely as possible.

At the same time, emerging technologies—particularly in cyber, AI, and space—must be part of any modern deterrence strategy. Future conflicts may not start with missiles but with data breaches, disinformation, or attacks on satellite infrastructure. The U.S. and

its allies need to be able to detect, deter, and respond across this full spectrum of threats.

Looking Ahead

The Indo-Pacific security environment isn't going to get any simpler. If anything, the region will continue to be a proving ground for how well the U.S. and its allies can adapt to 21st-century deterrence challenges. The concept of secondary decision centers is just one of many tools that may shape the future of U.S. strategy. Used wisely, they could add strength and flexibility to the alliance system. But they also demand a higher level of trust, coordination, and shared vision than ever before.

The discussions at the CGSR colloquium made one thing clear: the old playbook for deterrence is no longer enough. What's needed now is a dynamic, integrated approach that brings together not just military might, but also political will, technological innovation, and strong partnerships. In a world where threats are increasingly hybrid and unpredictable, adaptability is the cornerstone of effective deterrence.

Disclaimer: *All opinions in this article are solely those of the author and do not represent any organization.*