Integrated Deterrence and US Defense Strategy in NATO and AUKUS

An Analysis of Advanced Technologies and Multi-Domain Operations in Alliance Systems

Dr. Chris Dolan

Abstract

This article examines how integrated deterrence, multi-domain operations, and emerging technologies, particularly artificial intelligence (AI)—are reshaping US defense strategy in an era of complex and evolving threats. As adversaries enhance their military capabilities and exploit vulnerabilities across domains, the United States must leverage these elements to maintain strategic dominance and deter aggression. This analysis explores the role of advanced technologies in strengthening US defense alliances and security partnerships, particularly within NATO and the Australia–United Kingdom–United States (AUKUS) framework. By assessing the integration of AI, cyber capabilities, and multi-domain coordination, the article evaluates how these evolving strategies enhance interoperability, force readiness, and rapid response mechanisms. It highlights the extent to which a modernized US defense posture is adapting to counter peer and near-peer threats in an increasingly contested global security environment.

***

A rapidly evolving international security landscape demands swift modernization of US strategic deterrence and defense capabilities. To maintain military superiority and deter both state and nonstate adversaries, Washington must seamlessly integrate deterrence strategies, multi-domain operations (MDO), and emerging technologies. Artificial intelligence and machine learning (AI/ML), advanced cyber defenses, autonomous systems, and quantum technologies now define the next frontier of warfare.

The People's Republic of China (PRC), Russia, North Korea, Iran, and various nonstate actors continue to challenge US interests, forcing a reassessment of America's strategic posture within the North Atlantic Treaty Organization (NATO) and the Australia–United Kingdom–United States (AUKUS) defense partnership. Integrated deterrence, MDOs, and emerging technologies provide the best means to counter evolving threats, secure critical infrastructure, and protect space assets.

This article examines how these factors are reshaping US defense strategy within NATO and AUKUS. It assesses the threats posed by strategic competitors and evaluates how Washington sustains its military edge amid great-power competition.

The analysis focuses on the intersection of new strategic concepts and emerging technologies, emphasizing their application within alliance frameworks.

The discussion begins with a review of deterrence theory, tracing its evolution from classical deterrence through extended deterrence, escalation dominance, denial strategies, and integrated deterrence. It then analyzes how MDOs and emerging technologies influence US defense strategy. Next, it dissects the integrated deterrence framework, detailing its key components: critical technologies, MDOs, adversarial behavior, and the role of US allies and partners. The article then examines how US adversaries align their strategies to challenge American interests. Finally, it applies the integrated deterrence framework to US defense strategy within NATO and AUKUS, offering a comprehensive assessment of how these alliances adapt to modern warfare.

Deterrence Literature

Deterrence operates on a simple premise: the credible threat of consequences dissuades adversaries from pursuing harmful or undesirable actions. Over time, US national security strategy has adapted deterrence theory, shifting from classical models to extended, denial-based, escalation-dominance, and integrated approaches. No longer bound by Cold War-era paradigms, modern deterrence fuses critical technologies, accounts for the influence of both state and nonstate actors and incorporates MDOs into strategic planning.

During the Cold War, deterrence rested on signaling strength and demonstrating unified resolve—primarily to counter the Soviet Union. Thomas Schelling argued that deterrence hinges on coercion, compelling adversaries to alter their course by imposing costs or threatening punishment.[1] US strategy relied on overwhelming military force, with nuclear retaliation serving as the ultimate deterrent.[2] Mutually Assured Destruction (MAD) reinforced the notion that deterrence succeeds when an adversary perceives escalation as too costly to pursue.

Yet classical deterrence theory, while foundational, does not operate in a vacuum. Domestic politics, economic constraints, and bureaucratic inertia shape its effectiveness. Deterrence depends not only on the credibility of threats but also on an acute understanding of an adversary's strategic calculus. The structure of the international system, whether unipolar, bipolar, or multipolar—dictates deterrence's scope and the limits of its application.

[1] Thomas Schelling, *Arms, and Influence* (New Haven, CT: Yale University Press, 1967).
[2] Glenn H. Snyder, *Deterrence and Defense* (Princeton, NJ: Princeton University Press, 1961).

Extended deterrence, which broadens US security commitments to allies and partners, demands even greater credibility. It rests on the principle that unwavering and demonstrable commitments sustain alliance cohesion against militarily capable adversaries.[3] To deter aggression against its allies, the United States extends its nuclear umbrella, deploys forward-based conventional forces, and signals its readiness to incur risk and expend resources for collective defense.[4] Extended deterrence serves a dual purpose: it dissuades adversaries from testing US resolve while reassuring allies, thereby reducing the likelihood that they will pursue their own weapons of mass destruction.

Article 5 of the North Atlantic Treaty embodies extended deterrence, dissuading adversaries—once the Soviet Union, now Russia—from upending the balance of power. By extending the US security umbrella to vulnerable European allies, NATO signals that an attack on one member triggers a collective response, including US military action.[5] The alliance maintains this credibility through a mix of conventional forces, nuclear capabilities, strategic messaging, and democratic solidarity.[6]

Today, forward-deployed US troops, joint exercises, and NATO's nuclear-sharing arrangements serve as visible demonstrations of alliance resolve.[7] These measures take on heightened importance in the face of Russian aggression—first with the illegal annexation of Crimea, then with the full-scale invasion of Ukraine. The objective remains clear: convince Moscow that military action against a NATO member carries costs that vastly outweigh any perceived benefits. NATO's extended deterrence hinges on an unambiguous US commitment and unwavering transatlantic unity.

Yet extended deterrence is only as strong as the perception of its credibility. Any sign of wavering US commitment or fractures within NATO invites adversarial exploitation. Moreover, extended deterrence carries inherent risks—entangling the

---

[3] Joshua D. Kertzer, Jonathan Renshon, and Keren Yarhi-Milo, "How Do Observers Assess Resolve?," *British Journal of Political Science* 51, no. 1 (2021): 308–30, https://doi.org/.

[4] Matthew Fuhrmann and Todd D. Sechser, "Signaling Alliance Commitments: Hand-Tying and Sunk Costs in Extended Nuclear Deterrence," *American Journal of Political Science* 58, no. 4 (2014): 919–35, https://www.jstor.org/; and Paul K. Huth, "The Extended Deterrent Value of Nuclear Weapons," *Journal of Conflict Resolution* 34, no. 2 (1990): 270–90, https://doi.org/.

[5] Hugh Faringdon, *Strategic Geography: NATO, The Warsaw Pact, and the Superpowers* (New York: Routledge, 1989).

[6] Paolo Foradori, "European Perspectives," in *Tactical Nuclear Weapons and NATO*, ed. Tom Nichols, Douglas Stuart, and Jeffrey D. McCausland (Carlisle, PA; Army War College, Strategic Studies Institute, April 2012), 282–83.

[7] David Yost, "Assurance and U.S. Extended Deterrence in NATO," *International Affairs* 85, no. 4 (2009): 755–80, https://doi.org/.

US in unwanted conflicts or incentivizing free-riding behavior among allies.[8] If NATO members doubt US resolve, they may act recklessly, assuming Washington will back them regardless of their actions—a classic case of moral hazard.[9] Thus, sustaining alliance cohesion, modernizing military capabilities, restraining impulsive actors, and adapting to shifting threats remain paramount.

A key component of deterrence strategy is escalation dominance—the ability to control the spectrum of conflict at every level, from conventional skirmishes to nuclear brinkmanship. Effective deterrence does not simply rest on the threat of overwhelming force; it depends on an adversary's conviction that such force is usable and decisive.[10] Thomas Schelling's escalation ladder theory underscores this principle: the side that maintains control over escalation dynamics dictates the terms of conflict and deters opponents from believing they can gain an upper hand.[11]

However, escalation dominance is a double-edged sword. Mismanagement risks an escalation spiral—where provocation begets counter-provocation, leading to unintended war. Mastering escalation dominance requires a delicate balance: demonstrate strength, exercise restraint, and communicate clear consequences without leaving the adversary feeling trapped.[12] Without these elements, deterrence loses its potency, and stability erodes.

Deterrence has grown increasingly complex in an era defined by hybrid warfare, nonstate actors, cyberattacks, and rapid technological advances. In response, deterrence by denial emphasizes strengthening defensive capabilities to render adversarial aggression futile.[13] This approach convinces adversaries that hostile actions will fail to achieve their objectives, thereby making aggression strategically meaningless.[14]

---

[8] Thomas Plümper and Eric Neumayer, "Free riding in alliances: Testing an old theory with a new method," *Conflict Management and Peace Science* 32, no. 3 (2015): 247–68, https://doi.org/.

[9] Brett V. Benson, Adam Meirowitz, and Kristopher W. Ramsay, "Inducing Deterrence through Moral Hazard in Alliance Contracts," *Journal of Conflict Resolution* 58, no. 2 (2014): 307–35, https://doi.org/.

[10] Robert Ross, "Navigating the Taiwan Strait: Deterrence, Escalation Dominance, and U.S.-China Relations," *International Security* 27, no. 2 (2002): 48–85, https://doi.org/.

[11] Herman Kahn, *On Escalation: Metaphors and Scenarios* (New York: Routledge, 2009).

[12] Michael Fitzsimmons, "The False Allure of Escalation Dominance," *War on the Rocks*, 16 November 2017, https://warontherocks.com/.

[13] Kayse Jansen, "New Strategic Deterrence Frameworks for Modern-Day Challenges," *Joint Force Quarterly* 112, no. 1 (2024): 60–69; and T.V. Paul, "Complex Deterrence: An Introduction," in *Complex Deterrence: Strategy in the Golden Age*, ed. T. V. Paul, Patrick M. Morgan, and James J. Wirtz (Chicago: University of Chicago Press, 2009).

[14] Amir Lupovici, "Deterrence through Inflicting Costs: Between Deterrence by Punishment and Deterrence by Denial," *International Studies Review* 25, no. 3 (2023): 624–41, https://doi.org/; and Samuel Zilincik and Tim Sweijs, "Beyond deterrence: Reconceptualizing denial strategies and rethinking their emotional effects," *Contemporary Security Policy* 44, no. 2 (2023): 248–75, https://doi.org/.

Denial-based deterrence relies on hardening critical infrastructure, enhancing cyber and physical resilience, and reinforcing protective capabilities to dissuade aggression.[15] The logic is straightforward: an adversary will abandon hostile designs if success appears unattainable. Colby underscores this strategy's relevance in domains where attribution is difficult or retaliatory options are constrained—such as cyberwarfare or conflicts involving nonstate actors.[16] However, deterrence by denial is not without its weaknesses. It implicitly assumes that complete invulnerability is achievable—a problematic notion in an era of persistent cyberthreats and adaptive adversaries. Moreover, denial strategies depend on an adversary's internal assessment of vulnerabilities rather than an explicit threat of retaliation, making them potentially less credible than punishment-based deterrence.

Recognizing these challenges, policymakers have embraced integrated deterrence as the dominant strategic paradigm. This framework accounts for MDOs, interoperability with allies and partners, and the flexibility needed to counter threats from state and nonstate actors, cyberattacks, and disinformation campaigns.[17] Integrated deterrence adapts deterrence theory to the realities of modern conflict.[18] Given the resurgence of revisionist powers and the accelerating reliance on AI-driven warfare, resilient information networks and technological superiority will determine strategic advantage. The United States must harness its full range of military and technological assets to fortify critical systems, enhance cyber resilience, and institutionalize intelligence-sharing frameworks that mitigate the impact of disruptive attacks.[19]

Deterrence theory has evolved significantly since Schelling's foundational work. Classical deterrence provided a framework for rational actors, while extended deterrence broadened the concept to include allied security. Escalation and denial theories refined deterrence strategy by incorporating conflict dynamics, adversarial intent, and defensive capabilities. Today, scholars and policy makers must grapple with the challenge of deterring asymmetric warfare while maintaining decision dominance in battlespaces shaped by AI, autonomous systems, and hypersonic weapons. These realities demand a reassessment of deterrence frameworks—one that integrates all

[15] Alex S. Wilner and Andreas Wenger, *Deterrence by Denial: Theory and Practice* (New York: Cambria, 2021).

[16] Elbridge Colby, *The Strategy of Denial: American Defense in an Age of Great Power Conflict* (New Haven, CT: Yale University, 2022.

[17] Andrés J. Gannon, "One if by Land, and Two if by Sea: Cross-Domain Contests and the Escalation of International Crises," *International Studies Quarterly* 66, no. 4 (2022): 1–11, https://doi.org/.

[18] Patrick M. Morgan, "The Past and Future of Deterrence Theory," in *Cross-Domain Deterrence: Strategy in an Era of Complexity*, ed. Jon R. Lindsay and Eric Gartzke (New York: Oxford University Press, 2019); and Adam Mount and Pranay Vaddi, *An Integrated Approach to Deterrence Posture: Reviewing Conventional and Nuclear Forces in a National Defense Strategy* (Washington: Federation of American Scientists, 2021).

[19] Robert Chesney and Max Smeets, *Deter, Disrupt, or Deceive: Assessing Cyber Conflict as an Intelligence Contest* (Washington: Georgetown University Press, 2023).

elements of national power and international partnerships to sustain a credible and adaptive deterrent posture.[20]

The Integrated Deterrence Framework

Integrated deterrence strengthens military, diplomatic, economic, and technological capabilities by leveraging alliances and partnerships to dissuade adversaries.[21] Unlike traditional deterrence, which primarily relied on conventional military superiority, integrated deterrence emphasizes cross-domain coordination and multi-domain operations (MDOs).[22] It expands beyond military power to incorporate diplomatic pressure, information warfare, cybersecurity, financial instruments, intelligence cooperation, law enforcement, and homeland security.[23] This approach prioritizes working within established alliances such as NATO while forging new security arrangements like AUKUS. Unlike the uniform, one-size-fits-all framework of classical deterrence, integrated deterrence tailor strategies to specific adversaries, threats, and geopolitical contexts.[24]

The *2023 National Defense Strategy* underscores the importance of integrated deterrence, highlighting its application across land, air, sea, space, cyber, and information domains. It goes beyond conventional capabilities by incorporating artificial intelligence, machine learning, quantum computing, and autonomous systems to enhance decision-making speed and operational precision. However, integrated deterrence cannot function in isolation. Its success hinges on coordination across national security agencies, military branches, and allied nations. By increasing adversaries' operational and tactical dilemmas, integrated deterrence denies them opportunities to exploit vulnerabilities or undermine US security.[25] As adversaries adapt their physical and cyber strategies, defense planners must embrace integrated deterrence as a practical and necessary approach to contemporary security challenges.[26]

---

[20] Rebecca K.C. Hersman and Reja Younis, *The Adversary Gets a Vote: Advanced Situational Awareness and Implications for Integrated Deterrence in an Era of Great Power Competition* (Washington: Center for Strategic & International Studies, 2021); and James J. Wirtz and Jeffrey A. Larsen, "Wanted: a strategy to integrate deterrence," *Defense & Security Analysis* 40 no. 3 (2024): 361–78, https://doi.org/.

[21] Wirtz and Larsen, "Wanted," 362–63.

[22] Morgan, "The Past and Future of Deterrence Theory," 53.

[23] Steve Ferenzi and Robert C. Jones, "Three Ways to improve Integrated Deterrence," *National Interest,* 22 July 2022, https://nationalinterest.org/; and Gannon, "One if by Land, and Two if by Sea," 7.

[24] James Van de Velde, "Cyber Deterrence is Dead Long Live 'Integrated Deterrence," *Joint Forces Quarterly* 109 no. 2 (2023): 42–50.

[25] Michael Mazarr and Ivana Ke, "Integrated Deterrence as a Defense Planning Concept," *RAND*, 4 June 2024, 1–36, https://www.rand.org/.

[26] Matthew Olay, "Integrated Deterrence Is Key to Meeting Challenge of Future Conflicts, Brown Says," *DOD News*, 14 August 2024, https://www.defense.gov/.

Advanced Technologies and Cross-Domain Operations

At the core of integrated deterrence lies a suite of advanced technologies that expand military and strategic capabilities beyond the limits of traditional deterrence. Investments in hypersonic weapons, quantum computing, and biotechnology provide the United States with a decisive edge over adversaries, compelling them to recalibrate their strategies. Artificial intelligence (AI) and machine learning (ML) tools further enhance US and allied defense planning by streamlining coordination, breaking down institutional silos, and accelerating decision-making processes. AI-driven intelligence collection and data analysis improve situational awareness and threat detection, allowing military planners to anticipate and counter adversary actions with greater speed and precision. Quantum computing, in turn, strengthens encryption and fortifies critical communication systems against cyber threats.

AI and ML do more than refine decision-making—they revolutionize operational capabilities and strategic communication across multiple domains. By accelerating the Observe-Orient-Decide-Act (OODA) loop, these tools enable real-time threat monitoring, adversary behavior modeling, and rapid data analysis. They serve as force multipliers by enhancing precision targeting, attribution capabilities, and situational awareness.[27] AI also optimizes cross-domain coordination, integrating advanced battle management systems within command, control, communications, intelligence, surveillance, and reconnaissance (C3ISR) networks.[28] Moreover, AI-driven platforms enhance geolocation targeting and bolster defenses against hybrid threats.[29]

However, the same technologies that bolster deterrence also present vulnerabilities. Cyber-enabled warfare introduces what Schneider terms the "capability-vulnerability paradox"—the notion that as technological capabilities expand, so too do the risks of exploitation.[30] While cloud computing improves scalability and operational efficiency, infrastructure weaknesses create openings for state-sponsored cybercriminals to access classified and proprietary data. Quantum computing, despite its security benefits, also threatens to break encrypted communications, exposing sensitive intelligence to adversarial exploitation. To mitigate these risks, defense planners must

---

[27] Joseph L. Billingsley, *Integrated Deterrence and Cyberspace: Selected Essays Exploring the Role of Cyber Operations in the Pursuit of National Interest* (Washington: National Defense University Press, 2023).

[28] James Johnson, "Revisiting the 'stability–instability paradox' in AI-enabled warfare: A modern-day Promethean tragedy under the nuclear shadow?," *Review of International Studies* (November 2024): 1–19, https://doi.org/.

[29] Tim Stewart, "AI and the OODA loop: How AI enhances strategic decisions for today's warfighters," *Military Embedded Systems*, 21 June 2024, https://militaryembedded.com/.

[30] Jacquelyn Schneider, "Digitally Enabled Warfare: The Capability-Vulnerability Index," *Center for a New American Century*, 29 August 2016, https://www.cnas.org/.

pair technological innovation with robust security protocols. Sophisticated cyber defenses, real-time threat detection, and well-trained specialists are essential to ensuring AI-driven systems remain resilient against adversarial manipulation and operational failures.

Cross-domain collaboration—integrating information across cyber, information, land, sea, and air—has never been more critical. The rise of irregular warfare in multi-domain battlespaces demands swift, informed decisions. This reality underscores the necessity of cross-domain solutions (CDS), which mitigate risk and provide the decisive edge in modern conflicts. CDS systems instantaneously process data, information, and message formats, ensuring secure access to real-time threat intelligence.[31] By circumventing barriers imposed by siloed networks and restricted communications, CDS enhances coordination among military branches, intelligence agencies, and allied governments.

All-Domain Operations Centers (ADOC) should replace single-domain centers, integrating kinetic and non-kinetic effects and synchronizing operations across multiple levels and domains.[32] At the tactical level, tactical cross-domain solutions (TCDS) enable real-time data processing and battlefield communication, linking sensors, platforms, and warfighters across units and commands.[33] Likewise, multi-enterprise spanning architecture (MESA) facilitates secure data transfers between organizations and personnel at varying clearance levels, shielding networks from leaks and hostile infiltration.[34]

In multinational operations, CDS fosters seamless intelligence sharing, secure collaboration, and real-time coordination through multi-level security (MLS) operations.[35] Nowhere is this more urgent than in Europe and the Indo-Pacific, where the PRC and Russia aggressively seek geopolitical and technological advantages over the United States and its allies. Stronger integration among NATO members and AUKUS partners enhances resilience and fortifies critical infrastructure.[36]

Yet, technological prowess alone is not enough. Bureaucratic inertia and interagency silos remain persistent threats to effective coordination. Without streamlined

---

[31] George Kamis, "Achieving Decision Dominance in a Multi-Domain Battle Space," *Security Insights* (blog), 17 September 2024, https://www.everfox.com/.

[32] Paul Bauman, *Cross-Domain Synergy in Joint Operations: Planner's Guide* (Washington: US Joint Staff, 14 January 2016), https://www.jcs.mil/.

[33] "Tactical Cross Domain Solutions (TACDS)," General Dynamics, 2025, https://gdmissionsystems.com/.

[34] Mark Dobrena, "Trusted Thin Client MESA—The Future of Secure Cross Domain Collaboration," *Security Insights* (blog), 6 February 2025, https://www.everfox.com/.

[35] Valtteri Vuorisalo and Yacine Zaitiri, "Multi-Level Security: Enabling the future of multinational military operations" *Defence IQ*, 6 April 2018, https://www.defenceiq.com/.

[36] Mazarr and Ke, "Integrated Deterrence as a Defense Planning Concept," 20.

cooperation between US agencies and allies, even the most advanced systems risk undercutting deterrence rather than reinforcing it.[37] Worse, emerging technologies introduce vulnerabilities that adversaries can exploit, compounding risk and uncertainty in conflict. AI and machine learning, now embedded in critical infrastructure, influence sectors as diverse as health care, finance, telecommunications, and transportation. Their cascading effects demand not only integration but also vigilance against hostile manipulation.

In addition, information warfare, cyberattacks, and the militarization of space are reshaping the strategic landscape, challenging traditional deterrence, and demanding more adaptive responses.[38] The space domain, once a sanctuary for civilian and military infrastructure alike, now faces an array of emerging threats—antisatellite weapons, signal jamming, electronic warfare, and cyber intrusions.[39] Integrated deterrence must account for this new reality, not only by strengthening cybersecurity and developing offensive cyber capabilities but also by deepening collaboration with allies and partners. Deterrence now hinges on an approach—identifying vulnerabilities, mitigating risks, and denying adversaries the ability to exploit weaknesses. In an era of relentless technological and geopolitical shifts, traditional deterrence models no longer suffice against sophisticated threats.[40]

Yet, technology alone does not guarantee security. The human element remains the linchpin of integrated deterrence. Defense planners must articulate a coherent strategic vision, coordinate multi-domain operations, foster collaboration, and adapt to evolving threats. Effective decision-making requires a deep grasp of both technological capabilities and geopolitical realities. As military systems become increasingly automated, the role of the human operator grows even more critical. Machines execute, but people interpret. Only human judgment can navigate geopolitical pressures, craft innovative responses, and intervene when automation fails.

Most important, training and professional development must reinforce human expertise in managing emerging threats. Personnel must recognize cognitive biases in threat assessments, manage stress in high-stakes environments, and grasp the cultural and historical underpinnings of adversary behavior. Integrated deterrence does not rest on technology alone—it depends on the competence, agility, and leadership of those who wield it.

---

[37] Erik Gartzke and Jon Lindsay, "The U.S. Department of Deterrence," *War on the Rocks*, 22 July 2024, https://warontherocks.com/.

[38] Mazarr and Ke, "Integrated Deterrence as a Defense Planning Concept," 21.

[39] Mazarr and Ke, "Integrated Deterrence as a Defense Planning Concept," 22.

[40] Billingsley, *Integrated Deterrence and Cyberspace*, 46.

Axis of Adversaries

The resurgence of great power competition has crystallized into an axis of adversaries—The PRC, Russia, Iran, and North Korea—each committed to undermining American security and reshaping the global order to its advantage.[41] These revisionist states do not merely challenge US influence; they seek to dismantle it. Their shared objective is clear: weaken American power, erode its alliances, and rewrite the rules of the international system.

The strategic alignment between The PRC and Russia is neither new nor incidental. It has been in motion since Russia's 2014 annexation of Crimea, accelerating into what Velina Tchakarova has termed the "DragonBear" alliance—an enduring partnership that fuses military, diplomatic, economic, and technological ambitions.[42] This cooperation has deepened into a "no limits" pact, reinforcing their military and economic ties in a direct challenge to the United States and its allies.[43]

Against the PRC, the United States must employ integrated deterrence to reinforce AUKUS and strengthen NATO's alignment against Beijing.[44] The strategy extends beyond military posturing—it demands robust defenses against the PRC's cyber onslaught. The PRC state-sponsored hacking group Volt Typhoon has repeatedly attacked US critical infrastructure, government agencies, and private industry and Salt Typhoon breached critical infrastructure as well as communications devices of presidential election candidates in 2024.[45] More recently, the state-sponsored group APT27 has attacked US government agencies, the defense and energy sectors, and even targeted the Naval Academy and the Naval War College's China Maritime Studies Institute in a 2020 spear-phishing campaign.[46]

---

[41] Ronald O'Rourke, *Great Power Competition: Implications for Defense—Issues for Congress* (Washington: Congressional Research Service, 28 August 2024), https://sgp.fas.org/.

[42] Velina Tchakarova, "Considering the Dragonbear," *Central European Institute for Asian Studies*, 7 August 2019, https://ceias.eu/.

[43] Clara Fong and Will Merrow, "Where the China-Russia Partnership Is Headed in Seven Charts and Maps," *Council on Foreign Relations*, 12 December 2024, https://www.cfr.org/; and Andrea Kendall-Taylor and David O. Shullman, "Best and Bosom Friends: Why China-Russia Ties Will Deepen after Russia's War on Ukraine," *Center for Strategic and International Studies*, 22 June 2022, https://www.csis.org/.

[44] Bruce Jones et al., "Around the Halls: AUKUS defines an emerging alliance at sea," *Brookings*, 15 March 2023, https://www.brookings.edu/; and Patricia Kim et al., "The China-Russia relationship and threats to vital US interests," *Brookings*, 16 December 2024, https://www.brookings.edu/.

[45] "China Strategically Infiltrates U.S. Critical Infrastructure as Cyberattacks Escalate," *Soufan Center*, 10 January 2025, https://thesoufancenter.org/.

[46] "Justice Department Charges 12 Chinese Contract Hackers and Law Enforcement Officers in Global Computer Intrusion Campaigns" (press release, US Department of Justice, 5 March 2025), https://www.justice.gov/.

The threat is no longer theoretical. It is systemic. The challenge before the United States is not just countering an emboldened PRC but confronting a coordinated, revisionist bloc that exploits cyberwarfare, economic coercion, and military expansion to erode American dominance. The response must be equally strategic—integrating allies, reinforcing technological superiority, and dismantling adversarial networks before they achieve their objectives.

MDOs are central to countering the PRC. Deeper US force integration with Australia, the United Kingdom, Japan, and South Korea—through joint military exercises and interoperability drills—reinforces deterrence and strengthens allied resolve. Expanding maritime capabilities in the South China Sea and Taiwan Strait, backed by modern naval forces, signals unequivocally that the United States intends to stay in the region, defend its allies, and check Beijing's territorial ambitions. AI-enabled autonomous systems and maritime reconnaissance enhance situational awareness in the Indo-Pacific, improving threat prediction in strategic zones. Presence matters—but so does technological superiority.

Russia's actions confirm what was already evident: brute force remains central to its strategy. The illegal annexation of Crimea in 2014 and the full-scale invasion of Ukraine in 2022 reveal a playbook that combines hard military power with gray-zone tactics to undermine NATO and reassert Moscow's influence.[47] Hybrid warfare is the Kremlin's weapon of choice—blending cyber operations, disinformation, and frozen conflicts to destabilize nations. Moldova's Transnistria, Serbia–Kosovo tensions, and political dysfunction in Bosnia and Herzegovina are all case studies in Russia's strategy: disrupt, divide, and delay NATO and EU integration.[48]

Moscow's cyberwarfare extends beyond Europe. Russian-backed hackers have repeatedly targeted US critical infrastructure. In 2020, they compromised SolarWinds, embedding malicious code in software updates that penetrated US government agencies and private firms.[49] A year later, the Russian-backed group DarkSide launched a ransomware attack on Colonial Pipeline, crippling fuel supplies and exposing glaring vulnerabilities in the US energy sector.[50] Meanwhile, Russia's GRU

---

[47] Anita Parlow, "Hybrid War and National Security: NATO, the US, and the West," *The Russia File* (blog) 8 November 2024, https://www.wilsoncenter.org/.

[48] Rym Momtaz, "Taking the Pulse: Are Information Operations Russia's Most Potent Weapon Against Europe?" *Carnegie Endowment for International Peace*, 5 December 2024, https://carnegieendowment.org/.

[49] Vijay A. D'Souza, "SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response (infographic)," *WatchBlog* (blog), 22 April 2021, https://www.gao.gov/.

[50] Jennifer Easterly and Tim Fanning, "The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years," Cybersecurity and Infrastructure Security Agency, 7 May 2023, https://www.cisa.gov/.

intelligence unit, 29155, continues to conduct cyberespionage, industrial sabotage, and network infiltrations against US and NATO infrastructure.[51]

The stakes are clear. The PRC and Russia are not merely regional threats—they are revisionist powers methodically eroding US influence. Meeting this challenge requires more than just presence demands strategy, resilience, and the willingness to confront adversaries before they dictate the terms of engagement.

Secured AI tools and predictive analytics are critical to strengthening situational awareness and countering Russian aggression in Eastern Europe. Advanced systems can identify and analyze Russian military operations and communications with unprecedented speed and accuracy. Primer AI, for instance, processes Russian radio transmissions in real time, extracting sensitive intelligence with efficiency.[52] Using large-language models (LLM), it deciphers Russian military communications, enhancing visibility into troop movements and equipment deployments. Neural networks further integrate imagery intelligence from unmanned aerial vehicles, satellites, and ground-based sensors, accelerating analysis and producing more precise intelligence assessments.[53] AI-enabled tools leverage open-source intelligence (OSINT) to track Russian disinformation and monitor social media narratives.[54] In the information domain, speed is a weapon.

Tracking and countering Russian cyberoperations will grow even more critical as the PRC deepens its technological partnership with Moscow. Beijing and Moscow are now collaborating on AI, space-based military applications, and nuclear energy.[55] Huawei has embedded itself in Russian research institutions, testing quantum communication encryption systems.[56] In space, the PRC and Russia have pledged to develop a permanent lunar research station and an automated nuclear reactor on the moon—an unprecedented escalation in dual-use space technology.[57] On the nuclear front, Beijing and Moscow have signed agree-

[51] "NSA, FBI, CISA, and Allies Issue Advisory about Russian Military Cyber Actors" (press release, National Security Agency, 5 September 2024, https://www.nsa.gov/.

[52] Sean Gourley, "A New Era of Warfare: How AI Unlocks Intelligence from Russian Radio Chatter in Minutes," *Primer AI*, 4 April 2022, https://primer.ai/.

[53] Samuel Bendett, "Roles and Implications of AI in the Russian Ukrainian Conflict," *Center for a New American Security*, 20 July 2023, https://www.cnas.org/.

[54] Maya Sobchuk, "How Ukraine Uses AI to Fight Russian Information Operations." *Global Governance Institute*, 12 February 2024, https://www.globalgovernance.eu/.

[55] Kevin Pollpeter et al., *China-Russia Space Cooperation: The Strategic, Military, Diplomatic, and Economic Implications of a Growing Relationship* (Maxwell AFB, AL: China Aerospace Studies Institute, May 2023), https://www.cna.org/.

[56] Casey Babb, "A Match Made in Heaven: China-Russia Tech Cooperation and Canada's National Security," *Canada Global Affairs Institute*, March 2024, https://assets.nationbuilder.com/.

[57] Pollpeter et al., "China-Russia Space Cooperation."

ments worth USD 3.1 billion to build VVER-1200 reactors in the PRC while advancing joint research on fast breeder reactors and uranium-plutonium fuel cycles.[58] This is not mere cooperation—it is strategic alignment designed to challenge Western technological and military superiority.

The PRC's military buildup also relies heavily on Russian arms and defense technology. Moscow has supplied Beijing with missile systems, submarine technologies, Su-35 fighter jets, and advanced tanks. The People's Liberation Army (PLA) has acquired Russian avionics, engines, and radar systems while conducting joint military exercises with Russian forces.[59] Over the past decade, the PRC has purchased more than USD 39 billion in Russian arms, accounting for 77 percent of its total arms imports and significantly bolstering its military capabilities.[60] Meanwhile, Moscow and Tehran have become Beijing's primary energy suppliers. Despite Western sanctions, Iran continues to expand its energy exports to the PRC, supplying an estimated one million barrels of oil per day in 2023.[61]

The implications are clear. The PRC–Russia partnership is not a temporary alignment of convenience—it is a systematic effort to erode US influence, build military and technological alternatives to Western dominance, and reshape the global order. The United States must confront this reality with urgency, reinforcing deterrence, securing critical technologies, and ensuring that its adversaries do not dictate the terms of engagement.

Confronting Iran requires an unyielding strategy of integrated deterrence—sustaining sanctions on its nuclear program, countering cyber warfare, and disrupting its financial networks that sustain terrorism. Tehran continues to fund and arm foreign terrorist organizations, including Hezbollah, Hamas, and the Houthi rebels, while using energy revenues to prop up its regional ambitions. Iranian-backed cyber operatives have launched ransomware attacks against the US healthcare sector, targeted American financial institutions with distributed denial-of-service operations, and even hacked a dam in New York.[62] In the information space, Tehran has weaponized social media, spreading pro-Iranian

[58] Daniel Shats, *China-Russia Nuclear Industry Cooperation* (Maxwell AFB, AL: China Aerospace Studies Institute, January 2024), https://www.airuniversity.af.edu/.

[59] Yu-cheng Chen, "PLA Steps up Security Cooperation with Russia in 2024," *Jamestown Foundation*, 20 December 2024, https://jamestown.org/.

[60] Brian Carlson, "The Growing Significance of China-Russia Defense Cooperation," C*hina Landpower Studies Center*, 18 September 2024, https://ssi.armywarcollege.edu/.

[61] Kimberly Donovan and Maia Nikoladze, "The Axis of Evasion: Behind China's Oil Trade with Iran and Russia," *New Atlanticist* (blog), 28 March 2024, https://www.atlanticcouncil.org/.

[62] Evan Morgan, "Eroding Global Stability: The Cybersecurity Strategies of China, Russia, North Korea, And Iran," *Irregular Warfare Center*, 1 August 2024, https://irregularwarfare.org/.

propaganda in the aftermath of Hamas's October 7th terror attack on Israel. Iranian cyber sabotage extends beyond US borders—most notably in July 2022, when an Iranian operation crippled Albania's critical system, forcing the government to shut down public services.[63] Iran does not act alone; its digital and military provocations fit within a broader axis of adversarial cooperation.

North Korea remains a willing enabler of Russian military aggression, supplying Moscow with artillery shells and even troops for the war in Ukraine.[64] In return, Russia provides Pyongyang with advanced military technologies, including surface-to-air missiles, fighter jets, and ballistic missile systems.[65] More concerning, Moscow has signaled direct support for North Korea's satellite and space programs—initiatives with direct military applications that could further bolster Pyongyang's intercontinental ballistic missile (ICBM) capabilities.[66] The Kim regime's technological dependencies on Beijing and Moscow deepen the alignment between these authoritarian states, reinforcing a shared interest in undermining the US-led security order.

The strategic convergence of the PRC, Russia, Iran, and North Korea presents an unprecedented challenge to deterrence. These four regimes do not operate in isolation—they rely on each other to circumvent sanctions, share military technologies, and degrade US defense posture.[67] Their coordinated efforts risk fracturing NATO and AUKUS as US allies and partners weigh accommodations with an emerging geopolitical alternative. The consequences extend beyond conventional military threats—nuclear proliferation among these states is a growing risk and cyberattacks on US critical infrastructure could escalate.[68] Confronting this axis of revisionist powers requires an unshakable counterweight. NATO and AUKUS are not just military alliances; they are essential bulwarks against a world order shaped by adversaries hostile to US influence and global stability.[69]

---

[63] Magie Miller, "Albania weighed invoking NATO's Article 5 over Iranian cyberattack," *Politico*, 5 October 2022, https://www.politico.com/.

[64] Jim Garamone, "Austin Confirms North Korea Has Sent Troops to Russia," *DOD News*, 23 October 2024, https://www.defense.gov/.

[65] Edward Howell, "North Korea and Russia's Dangerous Partnership," *Chatham House*, 12 December 2024, https://www.chathamhouse.org/; and Soumya Narain and Bishwajit Acharya, "North Korea is the big beneficiary in its military partnership with Russia," *The Strategist*, 6 February 2024, https://www.aspistrategist.org.au/.

[66] Victor Cha and Ellen Kim, "The Fruits of Kim-Putin Summitry: North Korea's Military Satellite Launch," *Center for Strategic and International Studies*, 21 November 2023, https://www.csis.org/.

[67] Kim, et al., "The China-Russia relationship and threats."

[68] Stewart Lau, "China's Xi warns Putin not to use nuclear arms in Ukraine" *Politico*, 4 November 2024, https://www.politico.eu/.

[69] Chris Walsh and Joseph Kim, "Countering the China, Russia, Iran, North Korea Challenge," *George W. Bush Institute*, 12 January 2025, https://www.bushcenter.org/.

Implementation Challenges

Integrated deterrence relies on a fusion of military and technological capabilities to dissuade adversaries. Success demands seamless interoperability across cyber, information, land, sea, and air domains. Yet implementation challenges threaten to undermine these efforts.[70]

First, technological incompatibility impedes integration. Differing data formats, protocols, and standards create bottlenecks in communication, collaboration, and information sharing. Legacy systems, often incapable of interfacing with newer platforms, expose critical vulnerabilities that hostile state and nonstate actors will seek to exploit. Divergent security clearance levels among allies and partners further complicate intelligence-sharing and coordination.

Second, bureaucratic inertia and organizational fragmentation obstruct effective interoperability. Siloed network systems, controlled communication protocols, and competing institutional priorities hinder rapid responses to emerging threats. Poor command structures and misaligned defense investments among alliance members weaken collective deterrence. Burden-sharing remains a perennial challenge—allies may underinvest in their own defense, relying instead on the US security umbrella, thereby creating imbalances that strain alliance cohesion.[71] (Mallory et al. 2024).

Third, integrating AI/ML into military operations presents both opportunities and risks.[72] AI-driven platforms enhance situational awareness, refine human-machine interactions, and anticipate adversary behavior.[73] They accelerate the OODA loop, improving predictive analytics, data processing, and real-time threat identification. Advances in quantum computing further bolster encryption and secure communications.

Yet the capability-vulnerability paradox looms large. Enhanced efficiency does not always guarantee accuracy; shifting data streams can introduce bias into AI decision-making, undermining targeting, and high-end conflict preparation.[74] Cloud computing scalability, while a force multiplier, creates attack surfaces that state-backed cybercriminals could exploit to access classified information.

---

[70] Mazarr and Ke, "Integrated Deterrence as a Defense Planning Concept," 24.

[71] King Mallory et al., *Burden sharing and its Discontents: Understanding and Optimizing Allied Contributions to the Collective Defense* (Santa Monica: RAND, 7 May 2024), https://www.rand.org/.

[72] Kelsey Atherton, "Understanding the errors introduced by military AI applications," *Atlantic Council*, 6 May 2022, https://www.brookings.edu/.

[73] Wyatt Hoffman and Heeu Millie Kim, *Policy Brief: Reducing the Risks of Artificial Intelligence for Military Decision Advantage* (Wshington: Center for Security and Emerging Technology, March 2023), https://cset.georgetown.edu/.

[74] Alexander Blanchard and Laura Bruun, "Bias in Artificial Intelligence," *Stockholm International Peace Research Programme*, December 2024, https://www.sipri.org/; and Abigail Stowe-Thurston, "Open [AI] Skies," *New America*, 10 October 2023, https://www.newamerica.org/.

Integrated deterrence hinges on keeping human operators in the loop. Training defense and intelligence personnel to recognize AI/ML limitations and mitigate implementation failures is critical.[75] Cross-domain collaboration—merging intelligence from land, sea, air, space, and cyber domains—yields real-time situational awareness and adaptive targeting capabilities. These align with irregular warfare strategies that blend conventional and special operations forces to erode adversary legitimacy and sustain strategic advantage.[76]

NATO and AUKUS

US defense strategy operates differently within NATO and AUKUS, requiring distinct approaches to integrated deterrence and emerging threats in each multilateral framework. Both alliances recognize that technological and scientific innovation is critical to maintaining a strategic edge over Russia and the PRC.[77]

NATO, anchored in Article V's principle of collective security, is a formal alliance designed to deter Russian aggression against member states. US defense strategy within NATO's integrated deterrence framework spans conventional and nuclear capabilities alongside cyberoperations to prevent conflict. The transatlantic alliance prioritizes military readiness, force posture, and deterrence-by-denial strategies to counter Russian threats.

AUKUS, by contrast, is not a mutual defense treaty but a trilateral strategic partnership. It focuses on interoperability, intelligence-sharing, and advanced technological integration, particularly in nuclear submarine technology and military capability enhancement in the Indo-Pacific. The US role in AUKUS centers on deepening technological cooperation and fostering military and intelligence integration with Australia and the United Kingdom, laying the foundation for a long-term defense collaboration tailored to countering PRC expansionism.

NATO

NATO, established under the 1949 North Atlantic Treaty, is a broad-based alliance that integrates military and political strategies to uphold collective security, deter threats to member states, and reinforce transatlantic stability. Its deterrence posture spans multiple domains—including cyber, information, air, land, sea, and

[75] Michael Zequeira, "Artificial Intelligence as a Combat Multiplier: Using AI to Unburden Army Staffs," *Military Review*, September 2024, https://www.armyupress.army.mil/.

[76] Matthew Moellering, "Hiding in the Noise: Preparing the Irregular Warfare Community for the Age of AI," *Modern War Institute*, 26 September 2022, https://mwi.westpoint.edu/.

[77] John Hemmings, "AUKUS: Enhancing Undersea Deterrence," *Pacific Forum*, 26 May 2024, https://pacforum.org/.

space—to counter Russian aggression.[78] In response to Russia's 2022 invasion of Ukraine, NATO has prioritized Integrated Air and Missile Defense (IAMD) readiness, underscoring the importance of integration and interoperability across domains.[79] The interconnected nature of modern warfare means that attacks in one domain—whether physical or cyber—can cascade across military operations and critical infrastructure, making cross-domain resilience essential.

To sustain integrated deterrence, NATO's 32-member alliance requires seamless coordination. The alliance is expanding surveillance and sensor-to-shooter networks across unmanned aerial, ground, and maritime systems to enhance situational awareness and rapid-response capabilities.[80] NATO also maintains the CRONOS secure-messaging network to facilitate cross-domain military data-sharing, reinforcing operational cohesion.[81] These systems reflect NATO's commitment to collective defense and its adaptation to modern warfare's evolving threats.

Since Russia's full-scale invasion of Ukraine, NATO has accelerated investments in emerging and disruptive technologies (EDT), focusing on nine priority areas: AI, autonomous systems, quantum technologies, biotechnology, space, hypersonic systems, novel materials, energy and propulsion, and next-generation communications.[82] NATO's *2022 Strategic Concept* underscores the centrality of EDT initiatives. In 2021, NATO launched the Defence Innovation Accelerator for the North Atlantic (DIANA) to drive public-private and academic collaboration on defense innovations. DIANA funds accelerator sites and testing centers across member states, enabling scientists, engineers, industry experts, and procurement specialists to develop dual-use technologies, including advanced energy systems, autonomous undersea and aerial platforms, and secure data-sharing mechanisms.[83]

---

[78] Alina Polyakova et al., *A New Vision for the Transatlantic Alliance: The Future of European Security, the United States, and the World Order after Russia's War in Ukraine* (Washington: Center for European Policy Analysis, 30 November 2023), https://cepa.org/.

[79] "Deterrence and Defence," *North Atlantic Treaty Organization*, 13 December 2024, https://www.nato.int/.

[80] Franklin D. Kramer, Ann Marie Dailey, and Joslyn Brodfuehrer, "NATO multidomain operations: Near- and medium-term priority initiatives," *Atlantic Council*, 21 February 2024, https://www.atlanticcouncil.org/.

[81] *Optimizing Innovation Cooperation with Allies and Partners* (Washington: Defense Innovation Board, 2024), https://innovation.defense.gov/.

[82] Raquel Jorge Ricart, "NATO Defense Innovation and Deep Tech: Measuring Willingness and Effectiveness," *Carnegie Endowment for International Peace*, 29 August 2023, https://carnegieendowment.org/.

[83] "Defense Innovation Accelerator for the North Atlantic," North Atlantic Treaty Organization, https://www.diana.nato.int/; John Harper, "Latest NATO expansion includes massive increase in DIANA innovation accelerator sites," *Defense Scoop*, 15 March 2024, https://defensescoop.com/; and Amelia Kontesi, "Inaugural Dealroom and NATO Innovation Fund Report Reveals Record-Breaking Investing in Startups in European Defence, Security, and Resilience Sector," *Business Wire*, 12 February 2025, https://www.businesswire.com/.

NATO has launched initiatives and established new bodies to foster the development of innovative technologies aimed at countering external threats and challenges. Among these, the NATO Innovation Fund stands out as a USD 5.2 billion venture capital initiative focused on investing in start-ups developing dual-use technologies in defense, security, and resilience.[84] In 2022, NATO's defense ministers created the Data and Review Board (DARB), tasked with integrating operational guidelines for AI-sharing practices and promoting responsible AI adoption.[85] Additionally, the NATO Advisory Group on Emerging and Disruptive Technologies plays a critical role in guiding member states' technological innovation efforts. This group contributes to the development of strategic documents on a range of technologies, including biological and human enhancements, as well as quantum technologies.[86]

The Transatlantic Quantum Community (TQC) represents an informal but vital collaborative effort to advance quantum computing technologies. It encourages information and data sharing while strengthening quantum ecosystems. Experts from government, academia, and industry across NATO member states work together within this initiative to coordinate and manage the alliance's engagement with emerging technological trends, particularly in the realm of quantum technologies.[87]

Further bolstering these initiatives, NATO's Allied Command Transformation (ACT) serves as a central hub for transformation in military capabilities. ACT develops concepts for combined joint operations and support scientific research and technological development. The ACT also coordinates training programs among NATO allies and partner nations.[88] Meanwhile, NATO's Science for Peace and Security (SPS) program fosters international collaboration by integrating scientific innovation and information-sharing efforts. Through SPS, NATO provides both guidance and funding for technological initiatives, requiring that every multiyear grant-supported project involves collaboration between one NATO member and one partner country. These initiatives include workshops, training programs, and institutes.[89]

---

[84] Kontesi, "Inaugural Dealroom and NATO Innovation Fund Report."

[85] Daniel Fata, "NATO's Evolving Role in Developing AI Policy," *Center for Strategic and International Studies*, 8 November 2022, https://www.csis.org/.

[86] Simona Soare, "Innovation as Adaptation: NATO and Emerging Technologies," *German Marshall Fund*, 11 June 2021, https://www.gmfus.org/.

[87] Matt Swayne, "Updated AUKUS Pact Eases Export Controls on Quantum Among Member Nations" *Quantum Insider*, 20 August 2024, https://thequantuminsider.com/.

[88] Arnel P. David and Benjamin Jensen, "NATO and Prototyping Warfare," *Center for International and Strategic Studies*, 8 July 2024, https://www.csis.org/.

[89] "Science for Peace and Security," NATO, n.d., https://www.nato.int/.

Moreover, the NATO-Ukraine Innovation Cooperation Roadmap reflects Ukraine's adaptive and innovative efforts to incorporate advanced technologies in response to Russia's conventional military capabilities. This road map enhances interoperability between NATO and Ukraine by promoting technological innovation, ecosystem management, pilot programs, and the sharing of lessons learned.[90]

These collaborative initiatives are part of NATO's broader strategy to advance technological leadership. The alliance has made significant investments in AI, space-based defense systems, and cyber defense platforms, both cloud-based and on-site. In the space domain, NATO members have made space-based defense a core element of their integrated deterrence strategy, integrating antisatellite (ASAT) and nuclear detonation (NUDET) scenarios into their strategic planning and decision-making processes.[91] Additionally, NATO has prioritized the incorporation of AI into decision-making, situational awareness, and early warning systems. These advancements contribute to resilience measures designed to counter Russia's "Shadow War," which includes cyberattacks targeting critical infrastructure sectors in the West.[92] This includes efforts to disrupt military supply chains and integrated defense industrial bases.[93] By improving accuracy and efficiency, these programs significantly enhance real-time threat detection capabilities. However, to sustain these innovations, NATO must deepen its collaboration with the private sector to leverage open-source data and publicly available information, particularly to strengthen its cyber defense capabilities.

To streamline decision making and enhance coordination, NATO is equipping its multinational battlegroups with advanced command, control, communications, intelligence, surveillance, and reconnaissance (C3ISR) systems. These technologies probe for vulnerabilities and counter emerging threats with greater precision and agility. To strengthen command-and-control (C2) capabilities, NATO is integrating AI-enabled tools and prioritizing data-driven operational simulations, including all-domain models for training programs and concept development. Distributed ground command stations process intelligence gathered from surveillance and

---

[90] George Allison, "NATO Secretary General Emphasizes Commitment to Ukraine," *UK Defence Journal*, 20 June 2024, https://ukdefencejournal.org.uk/.

[91] Eugene C. Richter, "Achieving Alliance Space Deterrence: A Proposal for NATO 'Space Defense" (master's thesis, Air University, 22 March 2024), https://www.spacecom.mil/.

[92] Seth Jones, "Russia's Shadow War Against the West," *Center for Strategic and International Studies*, 18 March 2025, https://www.csis.org/.

[93] Beyza Unal, "Cybersecurity of NATO's Space-based Strategic Assets," *Chatham House*, July 2019, https://www.chathamhouse.org/; and Elizabeth Gosselin-Malo, "NATO to update artificial intelligence strategy amid new threats," *C4ISR*, 30 November 2023, https://www.c4isrnet.com/.

reconnaissance platforms, enabling real-time data fusion for targeting and intelligence exploitation.[94]

This approach provides multinational battlegroups with a comprehensive operational vantage point across all domains, allowing for better assessments of battlefield impact. Such recalibration enhances maneuverability and ensures NATO forces can rapidly shift capabilities and resources across vast distances. In parallel, NATO Air Policing remains a critical component of alliance defense, safeguarding the airspace of member states, including those lacking fighter aircraft.[95] NATO also actively counters hybrid threats that fuse military and nonmilitary tactics—ranging from disinformation campaigns on social media to cyberattacks and economic coercion aimed at destabilizing member states. To combat these evolving challenges, NATO has established counter-hybrid warfare teams that assist allies in addressing threats that deliberately blur traditional military and civilian domains.[96]

Managing technological capabilities and military operations across NATO's 32-member alliance presents formidable challenges. Effective coordination means integrating security policies. In the absence of cohesive policy frameworks, NATO's broad array of partnerships, collaborative programs, and investment funds risk increasing inefficiencies. If outdated and overlapping platforms come online at different intervals, operational vulnerabilities could arise. Compounding this challenge, programs and funds align more closely with individual national security interests rather than NATO's overarching strategic mission, which upholds collective defense and equal membership among states. Even more concerning, NATO allocates only 1 to 2 percent of its budget to partnerships, severely limiting its capacity to build enduring security initiatives.[97] This financial constraint could weaken NATO's Allied Command Operations (ACO) and Allied Command Transformation (ACT), both of which are crucial to maintaining operational superiority. Given these challenges, NATO's military and civilian leadership must fully integrate capabilities across land, sea, air, space, cyber, and information domains to ensure continuous coordination and seamless operations.[98]

---

[94] Gordon B. "Skip" Davis, "The Future of NATO C4ISR: Assessment and Recommendations After Madrid," *Atlantic Council*, 16 March 2023, https://www.atlanticcouncil.org/.

[95] Andrea Gilli, Mauro Gilli, and Gorana Grgić, "NATO, multi domain operations and the future of the Atlantic Alliance," *Comparative Strategy*, 14 January 2025, https://research-repository.st-andrews.ac.uk/.

[96] "Countering Hybrid Threats," North Atlantic Treaty Organization, 7 May 2024, https://www.nato.int/.

[97] Nicolo Fasola, "Reforming and Enhancing Partnerships to Strengthen NATO's Strategic Posture," *US Army War College*, 21 November 2024, https://publications.armywarcollege.edu/.

[98] Andreas Marlow, Wilson C. Blythe, "Multi-Domain Warfighting in NATO The 1 German-Netherlands Corps View," *Military Review*, March 2022, https://www.armyupress.army.mil/.

AUKUS

Established in 2021 as an informal trilateral security partnership, AUKUS is designed to uphold a "free and open Indo-Pacific" and counter the PRC's growing influence in the region.[99] The defense framework is structured around two pillars. Pillar 1 strengthens Australia's maritime capabilities through a major investment in nuclear-powered submarines, a direct response to the PRC's expanding naval presence. Pillar 2 advances trilateral cooperation by enhancing integration, interoperability, and information-sharing across critical domains, including hypersonic weapons, artificial intelligence, cybersecurity, quantum technologies, undersea capabilities, electronic warfare, and defense innovation. Both pillars underscore the role of nuclear propulsion and next-generation defense technologies in bolstering deterrence against the PRC's regional ambitions.[100]

AUKUS functions less as a formal alliance and more as a strategic partnership aimed at reinforcing integrated deterrence against PRC power projection. Its objectives include expanding intelligence-sharing mechanisms, consolidating investments in advanced technologies, conducting joint military exercises, and ensuring interoperability across defense systems and platforms. Additionally, AUKUS seeks to align procurement strategies, integrate supply chains, and strengthen the three nations' defense industrial bases.[101] Through this heightened collaboration, the partnership enhances maritime operations and fortifies regional deterrence against the PRC's military modernization and territorial expansion. Unlike NATO, which operates as a collective defense alliance, AUKUS is a capabilities-based defense arrangement rooted in trust, mutual innovation, and technological cooperation. Its strategic value lies in the seamless integration of military capabilities and intelligence systems among the three partners.

Pillar 2's focus on hypersonic missile systems provides AUKUS with a formidable deterrent by reducing the PRC's reaction time to incoming threats, thereby reinforcing a more assertive posture in integrated deterrence. Hypersonic missiles—capable of exceeding Mach 5—offer enhanced precision and flexibility, granting AUKUS a strategic advantage in countering the PRC's air defense systems. The partnership's collaboration on hypersonic technology emphasizes the development of hypersonic

[99] Paul Wintour, "What is the AUKUS Alliance and What are its Implications?," *The Guardian*, 16 September 2021, https://www.theguardian.com/.

[100] Justin Bassi, Maeve Ryan, and Lisa Curtis, "AUKUS Is More Than Submarines: Its Advanced Capabilities Pillar Will Also Require Fundamental Shifts," *Just Security*, 10 July 2023, https://www.justsecurity.org/.

[101] Lauren Kahn, "AUKUS Explained: How Will the Trilateral Pact Shape Indo-Pacific Security?," *Council on Foreign Relations*, 12 June 2023, https://www.cfr.org/.

glide vehicles (HGV) and other cutting-edge weapons systems.[102] The AUKUS-integrated hypersonic weapons initiative includes the Hypersonic Flight Test and Experimentation (HyFliTE) Project Arrangement, a program designed to accelerate the testing and refinement of hypersonic vehicles.[103] Backed by a shared investment of USD 252 million, HyFliTE plans to conduct six test flights by 2028, leveraging common propulsion systems, high-temperature materials, guidance and control technologies, testing infrastructure, and industrial expertise across the three partner nations.[104] Through these efforts, AUKUS is advancing the Indo-Pacific's strategic landscape, positioning itself as a critical force in countering the PRC's regional ambitions.

AUKUS members are making substantial investments in Pillar 2's focus on AI-enabled tools to enhance precision targeting, autonomous weapons systems, and intelligence operations. For instance, to bolster antisubmarine warfare and improve submarine detection, trilateral AI algorithms are being developed for P-8A maritime patrol aircraft. These AI systems analyze sonobuoy data collected from Australian, British, and American sources, enhancing underwater threat detection and tracking capabilities.[105] AI technologies are also advancing multi-domain data collection, allowing commanders to integrate intelligence with greater speed and accuracy. The Resilient and Autonomous Artificial Intelligence Technologies (RAAIT) initiative is further integrating AI into force protection, intelligence gathering, targeting, and surveillance and reconnaissance operations.[106]

To accelerate progress in robotics and autonomous systems, AUKUS members have conducted extensive testing on ground and aerial autonomous drones, including the Blue Bear Ghost drone and Challenger 2 tanks.[107] In 2023, joint tests in Australia featured US and UK robotic ground vehicles, cross-domain launches, and unmanned platforms. That same year, an AI-enabled swarm test in the U.K. involved the Blue Bear Ghost drone, Challenger 2 tanks, Warrior armored vehicles,

[102] Justin Katz, "Hypersonics Too Expensive, Industrial Base Too Small For Services to Go It Alone: Admiral," *Breaking Defense*, 3 November 2022, https://breakingdefense.com/.

[103] Mikayla Easley, "AUKUS alliance seals plans for collaboration on hypersonics testing," *Defense Scoop*, 18 November 2024, https://defensescoop.com/.

[104] Katz, "Hypersonics Too Expensive, Industrial Base Too Small."

[105] Aaron Mehta, "P-8 'trilateral algorithm' to hit field this year, as AUKUS Pillar II eyes quantum clocks, AI projects," *Breaking Defense*, 29 May 2024, https://breakingdefense.com/.

[106] "AUKUS Pillar II Milestones Hint at Future Integrated Autonomous, Artificial Intelligence Operations" (press release, Department of Defense, 19 August 2024), https://www.defense.gov/.

[107] Tim Martin, "AI side of AUKUS: UK reveals ground-breaking, allied tech demo," *Breaking Defense*, 25 May 2023, https://breakingdefense.com/2023/05/the-ai-side-of-aukus-uk-reveals-ground-breaking-allied-tech-demo.

and Viking unmanned ground vehicles.[108] In 2024, Australia hosted joint exercises integrating autonomous platforms, unmanned aerial and underwater vehicles, and submarine-hunting sonobuoys.[109]

AUKUS members are also expanding subsea and seabed warfare capabilities to monitor and defend critical undersea infrastructure. To strengthen unmanned undersea operations, the partnership is developing submarine-launched unmanned underwater vehicles (UUV) and torpedo-tube launch-and-recovery (TTL&R) systems.[110] Additionally, the AUKUS Maritime Autonomy Experimentation and Exercise Series aims to improve interoperability in autonomous maritime systems, ensuring seamless coordination across allied naval forces.[111]

In cybersecurity, AUKUS is advancing joint cyber resilience initiatives, reinforcing supply-chain security, and expanding cooperative research and development programs. Real-time threat identification, continuous monitoring, vulnerability analysis, and cyber training remain key priorities.[112] To further enhance cybersecurity integration in naval supply chains, AUKUS is collaborating with private-sector suppliers to develop unified cybersecurity standards. These efforts emphasize technical capability integration, workforce training, and standardized certifications and accreditations. Moreover, joint research-and-development (R&D) initiatives are bringing together cyber threat experts from all three member states to accelerate cyber workforce development and strengthen advanced cyber capabilities.[113] Through these measures, AUKUS is not only enhancing deterrence but also fortifying its technological edge in the evolving security landscape of the Indo-Pacific.

AUKUS is making strategic investments in quantum technologies, focusing on research and development, standardization, export controls, and industry collaboration. Under the AUKUS Quantum Arrangement (AQuA), members are funding next-generation quantum computing initiatives to enhance navigation, timing, and positioning while accelerating innovation at scale. Specific applications include optical atomic clocks, quantum sensors for military platforms, and quantum-based

---

[108] Martin, "AI side of AUKUS."

[109] Alex Luck, "Australia, United Kingdom, United States Tout Drone Networks at Autonomous Warrior 2024," *Naval News*, 31 October 2024, https://www.navalnews.com/.

[110] Peter Suciu, "AUKUS Nuclear-Powered SSN Submarine Could be a Drone Mothership," *National Interest*, 17 April 2024, https://nationalinterest.org/.

[111] Luke A. Nicastro, *AUKUS Pillar 2 (Advanced Capabilities): Background and Issues for Congress* (Washington: Congressional Research Service, 21 May 2024), https://www.congress.gov/.

[112] Martin, "AI side of AUKUS."

[113] Nicastro, "AUKUS Pillar 2."

secure communications.[114] Also, AUKUS is developing shared policies and standards to govern the commercial, intelligence, and legal dimensions of quantum technologies and their military applications.[115] To sustain momentum in quantum development, AUKUS must ensure that export controls on sensitive technologies do not impede integration and interoperability.

In electronic warfare, AUKUS is implementing a data-sharing framework designed to enhance trilateral interoperability, with completion expected by 2025. This framework will facilitate cross-domain electronic warfare (EW) collaboration among the partners, enabling greater coordination in electromagnetic spectrum operations.[116] To support this effort, AUKUS has established the Electronic Warfare Innovation Challenge, which allocates funding to companies from all three member states to develop joint EW projects.[117] To further integrate capabilities across domains, AUKUS members are conducting joint exercises to assess and enhance EW effectiveness, strengthen industrial supply chains, and refine precision tracking, targeting, and electronic attack capabilities.[118]

AUKUS members are also advancing secure data-sharing frameworks to streamline defense industrial cooperation and intelligence coordination. A key initiative involves developing cloud-based platforms that enable classified information-sharing and facilitate AI and machine learning model development (Biden 2024). These platforms will support integration in both Pillar 1's nuclear propulsion efforts and Pillar 2's advanced cybersecurity, AI, quantum computing, and hypersonic missile development.[119] The objective is to create a secure and interoperable network that connects cleared military, intelligence, and industry personnel.

While AUKUS is a "minilateral" partnership centered on integrated deterrence against the PRC, NATO remains a collective security alliance committed to defend-

[114] Josh Luckenbaugh, "AUKUS Nations Making Inroads on Quantum Tech but Barriers Remain," *National Defense*, 21 February 2025, https://www.nationaldefensemagazine.org/.

[115] Susanne Lloyd-Jones and Kayleen Manwaring, "Quantum Resilience in the Australian National Security Legislative Framework (Policy Brief)," *University of New South Wales Law Research Paper* No. 24-32 (2024), http://dx.doi.org/.

[116] Carley Welch, "AUKUS partners to stand up electronic warfare intel-sharing framework," *Breaking Defense*, 14 November 2024, https://breakingdefense.com/.

[117] Brandi Vincent, "AUKUS shares results of inaugural Electronic Warfare Challenge," *Defense Scoop*, 26 September 2024, https://defensescoop.com/.

[118] Laura Heckman, "AUKUS Challenge Prize Propels Partners' Electronic Warfare Tech," *National Defense*, 13 March 2025, https://www.nationaldefensemagazine.org/.

[119] Nicastro, "AUKUS Pillar 2."; and Welch, "AUKUS partners to stand up."

ing its members against Russia.[120] AUKUS measures its progress through investments in joint defense technology projects, such as the AUKUS Quantum Arrangement and Resilient and Autonomous Artificial Intelligence Technologies initiative, as well as advancements in key military capabilities, including the Hypersonic Flight Test and Experimentation Project Arrangement and submarine-launched unmanned underwater vehicles with torpedo-tube launch-and-recovery systems. These initiatives not only enhance AUKUS's operational effectiveness but also reinforce its role as a technological force multiplier in the Indo-Pacific.

NATO possesses a far deeper institutional memory of integrated deterrence, having spent decades countering Russian aggression in the European security environment. In contrast, AUKUS is a more specialized and nascent partnership, focused on maritime and technological applications to counter the PRC in the Indo-Pacific. At its core, AUKUS hinges on interoperability across technologies, intelligence systems, cyber capabilities, and nuclear submarines. Australia, the United Kingdom, and the United States share mutual concerns over the PRC's rapid military modernization and territorial ambitions amid a shifting global order. However, unlike NATO, AUKUS lacks a formal collective security commitment among its members and remains in an early stage of development as a defense partnership.

AUKUS serves as a proving ground for integrated deterrence and cross-domain operations. Its effectiveness depends on the advancement and deployment of innovative technologies, enhanced intelligence and data sharing, and a shared strategic culture centered on maintaining a robust and resilient posture in the Indo-Pacific. Over time, AUKUS could expand to include additional partners, such as Canada, Japan, or New Zealand, or serve as a foundation for further bilateral or multilateral agreements aimed at strengthening integration and interoperability in the region.

Conclusion: Policy Implications and Recommendations

Based on the analysis presented, this article offers policy recommendations to enhance US defense capabilities and strengthen its integrated deterrence posture.

First, the United States must prioritize R&D investments in critical and emerging technologies across all domains of modern warfare. Accelerating innovation in AI/ML, quantum computing, advanced cybersecurity, space-based assets, and autonomous weapons systems are imperative. These advancements will secure US decision dominance as its primary adversaries—namely the PRC, Russia, North

[120] Courtney Stewart, "Think Bigger, Act Larger: A U.S.-Australia Led Coalition for a Combined Joint Deterrence Force in the Indo-Pacific," *Carnegie Endowment for International Peace*, 2 October 2024, https://carnegieendowment.org/.

Korea, Iran, and their affiliated nonstate actors—deepen collaboration to challenge US strategic interests. The Department of Defense (DOD) should establish dedicated task forces to explore military applications of innovative technologies and integrate them into existing defense platforms. This approach will bolster US military capabilities and deter adversaries from exploiting vulnerabilities within the US and allied defense frameworks.

Additionally, US defense planners must invest in intelligence capabilities to enhance situational awareness and better anticipate adversarial behavior. This requires funding innovative programs that improve accuracy in intelligence collection, human-machine teaming, and real-time data analysis. The DOD should expand partnerships with universities and defense corporations through basic research initiatives. The Army Research Office (ARO) within the US Army Combat Capabilities Development Command Army Research Laboratory (DEVCOM ARL) should increase funding for defense-related scientific advancements. Likewise, the Air Force Office of Scientific Research (AFOSR) should expand its calls for research proposals through the Air Force Research Laboratory (AFRL), while the Office of Naval Research (ONR) should enhance funding for critical maritime defense initiatives. Broad Agency Announcements (BAA) should also solicit research proposals from academia and industry to advance AI/ML-driven intelligence collection and analysis for the battlefield.

Second, the United States must deepen defense integration within alliances and security partnerships, as the effectiveness of deterrence depends on interoperability. The George C. Marshall Center for European Security Studies and the Defense Security Cooperation University play key roles in strengthening security cooperation, professional military education, and allied defense integration. The United States should increase support for these institutions while reinforcing NATO and AUKUS working groups focused on enhancing interoperability and secure data sharing. Coordinating closely with allies ensures that neither the PRC nor Russia achieves a military or technological edge over the United States and its partners. Furthermore, the DOD must align its integrated deterrence strategy—particularly MDOs and emerging military technologies—with the defense policies of allied and partner nations to facilitate coordinated responses to both state and nonstate threats. Multinational task forces and strategic dialogues will be essential in addressing regional security challenges and evolving cyberthreats.

Third, the DOD should prioritize cross-domain integration of defense capabilities across land, sea, air, space, cyber, and information environments. Strengthening collaboration between these domains will require upgrading C2 systems, enhancing joint operational concepts, and fostering cross-service coordination. Expanding the Irregular Warfare Center (IWC) to develop training initiatives focused on multi-domain

warfare is critical. Establishing joint commands dedicated to coordinating operations across military branches will further enhance integration. Additionally, US defense planners should collaborate with allies to develop shared multi-domain operational concepts and conduct joint exercises that refine these strategies in real-world scenarios.

Fourth, US national security planners must revise the *National Defense Strategy* (NDS) to emphasize whole-of-government collaboration in protecting critical infrastructure. Integrated deterrence requires a strong focus on both cyber and physical security, given that sophisticated state and nonstate actors continuously seek to exploit vulnerabilities. The NDS should prioritize deeper coordination with the Department of Homeland Security (DHS) and the Cybersecurity and Infrastructure Security Agency (CISA) to counter cyber threats targeting the US defense industrial base. Strengthening cyberthreat intelligence sharing, enhancing network security, and investing in workforce development will be essential in mitigating cascading cyber risks across critical sectors.

Fifth, NATO and AUKUS should collaborate to enhance the practical application of integrated deterrence. Closer coordination between these two security frameworks will empower the United States and its allies to develop a more cohesive deterrence posture while strengthening collective defense capabilities. Joint military exercises and intelligence-sharing mechanisms will help address mutual security threats, particularly as the PRC and Russia expand their military and technological cooperation. Cyber resilience efforts will be especially critical, given the increasing sophistication of nonstate cyber actors and the growing role of AI in multi-domain operations.

AUKUS's Pillar 2 provides a model for NATO to expand its focus beyond traditional defense structures and incorporate advanced technology-sharing initiatives to improve interoperability. While NATO's Article 5 commitment to collective security defines its core mission, member states must also invest in cyber and physical security integration to address vulnerabilities within critical infrastructure sectors. Promising initiatives such as the DIANA, the Data and Review Board, and the Transatlantic Quantum Community should be expanded to bolster technological collaboration. NATO and AUKUS should also establish joint task forces composed of military officials, industry experts, and academic researchers to enhance technology integration, intelligence-sharing, and strategic coordination. While NATO remains focused on transatlantic security and AUKUS on the Indo-Pacific, both frameworks can improve coordination through regular joint exercises, simulations, and strategic communications. These efforts will reinforce MDOs and integrated deterrence, particularly against hybrid warfare and cyber threats originating from state and nonstate actors. Establishing common standards for cybersecurity, AI/ML applications, and human-machine teaming will further enhance system interoperability and security.

Finally, integrated deterrence strategies must be tailored to the specific threats posed by state and nonstate adversaries. The current international system is defined by intensifying great power competition, with military capabilities and critical technologies serving as primary battlegrounds. A generic, one-size-fits-all deterrence framework is neither practical nor effective. While unified in their opposition to US strategic interests, the PRC, Russia, North Korea, and Iran each have distinct motivations and operational approaches. To sustain an effective deterrence posture, the United States and its allies must continuously assess the evolving capabilities and strategic objectives of these adversaries and their proxy networks.

Dr. Chris Dolan

Dr. Dolan is Assistant Teaching Professor of Homeland Security and Public Policy at the Pennsylvania State University at Harrisburg. His research focuses on homeland security and cyber defense, advanced defense technologies, cyberthreat intelligence, NATO, and critical infrastructure protection. In 2024, Dolan was a Fulbright State Department Specialist in cyber defense and critical infrastructure with the Kosovar Centre for Security Studies (KCSS) in Kosovo. He is also a two-time Fulbright US Scholar (North Macedonia, 2022; Kosovo, 2019–2020). In 2023, he published two books: *NATO, the U.S., and Cold War 2.0* and *The Politics of U.S. Foreign Policy and NATO*.

Disclaimer

The views and opinions expressed or implied in *Strategic Horizons* are those of the authors and should not be construed as carrying the official sanction of the Department of Defense, Department of the Air Force, Air Education and Training Command, Air University, or other agencies or departments of the US government or their international equivalents.