FUTURE UNCERTAIN: NATO IN A POST-QUANTUM, POST-AI WORLD

The emerging and disruptive technologies of the 21st century—artificial intelligence and quantum technologies—confront NATO with a paradox: the integration of those technologies into national armed forces will significantly narrow and possibly invert the systemic technology dominance NATO has enjoyed since 1945 and widen the technology gap within the Alliance with potentially debilitating consequences for operational effectives and allied cohesion. The precise impact of these disruptive technologies must remain largely speculative, but it is certain that they will change the nature of war-fighting, exacerbate the security dilemma, and precipitate in a recalibration of the global balance of power.

James Sperling*

TPQ
Summer 2022

* James Sperling is a Professor Emeritus of Political Science at the University of Akron.

The role of technological change in the conduct or warfare or consequential shifts in the balance of power is beyond dispute. Technological changes fall along spectrum bounded at one end by evolutionary changes with incremental modifications of doctrine and at the other by revolutionary changes that can initiate systemic change. The deployment of ICBMs with multiple independently maneuverable reentry vehicles (MIRVs) or nuclear capable cruise missiles initiated a shift in the offensive-defensive balance in ways that aggravated the security dilemma: both created a foundation for transitioning from a strategy of counter-value retaliation to a counter-force strategic first strike. Revolutionary technologies, by contrast, initiate a fundamental shift in the balance of power or render obsolete major military capabilities underpinning military doctrine: the introduction of gunpowder as a propellant and explosive in the 13th century and nuclear weapons in 1945 had such systemic consequences. The 21st century technologies are likely to include both categories of technological change; many, like artificial intelligence (AI) and quantum technologies, will not only alter the global and theatre correlation of forces between NATO and its adversaries, but may reshape the global balance of power.

These technologies may also create an unbridgeable technology gap within NATO. There has been a persistent technology gap within NATO since its founding which limited NATO's operational effectiveness and weakened Alliance cohesion.1 Today, NATO is preoccupied with the internal and external consequences of emerging and disruptive technologies (EDT): many fear that these technologies will minimize or erase NATO's decades-long technological edge vis-à-vis any peer competitor or potential adversary.2 NATO Secretary General Jens Stoltenberg summed up this shared concern in his 2020 *Annual Report*: "Technological dominance has always been key to NATO's success. But that dominance is now being challenged…" with potentially dire consequences for NATO's ability to protect its core and peripheral interests regionally and globally. These EDTs may also have the unintended consequence of exacerbating the decades-long technology gap between the U.S. and its allies—an outcome that would compound the loss of technological dominance.[3]

The *NATO 2022 Strategic Concept* reiterated that strategic concern: "[EDTs]… are altering the character of conflict, acquiring greater strategic importance, and

[1] Representative studies include Robert L. Pfaltzgraff, Jr., *The Atlantic Community: A complex imbalance* (New York: Von Nostrand Reinhold, 1969): p. 72-88; David Yost "The NATO Capabilities Gap and the European Union," *Survival*, Vol. 42, No. 4 (2000): p. 97-128; and William Greenwalt, *Leveraging the National Technology Industrial Base to Address Great-Power Competition: The Imperative to Integrate Industrial Capabilities of Close Allies* (Washington, DC: Atlantic Council, 2019).

[2] Leona Alleslev, *Defence Innovation: Special Report*, 041 STC 20 E rev. 1 (Brussels: NATO Parliamentary Assembly, 2020): para 8-16.

[3] NATO, *The Secretary General's Annual Report 2020* (Brussels: NATO, 2021): p. 54.

becoming key arenas of global competition. Technological primacy increasingly influences success on the battlefield."[4] The goal of technological primacy, in turn, yielded an intra-alliance agreement to "promote innovation and increase our investments in emerging and disruptive technologies to retain our interoperability and military edge."[5] The new strategic concept identified the Russian Federation and the People's Republic of China as NATO's contemporaneous and putative threats, respectively, to the alliance and its member states. Emerging technologies play a key role in shaping the NATO perception of the nature of the threats posed. In the Russian case, the document identified the deployment of "novel and disruptive dual-capable delivery systems" (i.e., hypersonic missiles and cruise missiles) that could lead to fundamental changes in nuclear doctrine and fatally compromise allied nuclear (and conventional) deterrence.[6] The immediate concerns with China are ongoing "malicious hybrid and cyber operations" against NATO member states, but the long-term threat was identified as China's long-term ambition to control "key technological and industrial sectors, critical infrastructure, and strategic materials and supply chains." If that goal were to be realized, China would offset or end NATO's existing margin of technological dominance.[7]

> *"Five of those technologies—artificial intelligence (AI), lethal autonomous weapons systems (LAWS), hypersonics, space, and quantum—are the most likely to disrupt strategic stability and reduced allied interoperability and cohesion."*

These concerns surrounding EDTs raise three interconnected questions: What EDTs are the most critical for NATO? How might the integration of technologies across the major warfighting (land, air, sea, and space) domains affect the offensive-defensive balance? What dangers do these EDTs pose for NATO's future interoperability and cohesion? The answers to those questions establish the range of technologically induced challenges NATO will face in the future.

[4] NATO, *NATO 2022 Strategic Concept, Adopted by Heads of State and Government at the NATO Summit in Madrid*, 29 June (Brussels: NATO, 2022), para 17, available at: https://www.nato.int/strategic-concept/

[5] NATO, *NATO 2022 Strategic Concept, Adopted by Heads of State and Government at the NATO Summit in Madrid*, 29 June (Brussels: NATO, 2022): para 24.

[6] NATO, *NATO 2022 Strategic Concept, Adopted by Heads of State and Government at the NATO Summit in Madrid*, 29 June (Brussels: NATO, 2022): para 8.

[7] NATO, *NATO 2022 Strategic Concept, Adopted by Heads of State and Government at the NATO Summit in Madrid*, 29 June (Brussels: NATO, 2022): para 13.

Emerging and Disruptive Technologies

The United States and NATO followed successive technology-driven strategies designed to substitute capital (advanced weapons systems) for labor (armed forces) to offset Warsaw Pact's quantitative superiority across weapons systems and personnel. These strategies, for example, included the introduction of tactical nuclear weapons in the 1950s and stealth technologies in the 1980s. The current offset strategy seeks to integrate quantum and artificial intelligence technologies into all military capabilities.[8] This offset strategy differs from those that came before it in at least two respects. First, a putative adversary—China—is acknowledged to be doing the same *and* is assumed capable of doing so to the detriment of NATO.[9] Second, quantum and artificial intelligence technologies will render virtually meaningless the distinction between offensive and defensive capabilities: the offensive or defensive purpose of an AI or quantum augmented weapons system can only be determined *ex post*. Moreover, these technologies currently favor the offense: swarm technologies and hypersonic (cruise) missiles make carrier task groups highly vulnerable to A2/AD strategies, while advances in quantum sensor technologies would irrevocably compromise a second-strike capability and, by extension, further erode the extended American deterrent underpinning NATO.[10]

What EDTs are the NATO Member States Seeking to Develop?

In 2021, NATO issued an EDT strategy identifying the critical technology clusters in the 21st century.[11] Five of those technologies—artificial intelligence (AI), lethal autonomous weapons systems (LAWS), hypersonics, space, and quantum—are the most likely to disrupt strategic stability and reduced allied interoperability and cohesion.

Quantum

Quantum technologies with military applications fall into three categories: communications, quantum, and computing. Quantum computers will enable comprehensive situational awareness across war-fighting domains and big

[8] On the evolution of these offset strategies, see Gabriele Rizzo, "Disruptive Technologies in Military Affairs" in Fabio Rugge (ed.), *The Global Race for Technological Superiority* (Milan: ISPI, 2019): p. 55-92. On the potential of quantum and AI technologies, see NATO ACT, "Military Uses of Artificial Intelligence, Automation, and Robotics (MUAAR),"-*Fact Sheet* (2020), at: https://www.act.nato.int/application/files/5515/8257/4725/2020_mcdc-muaar.pdf

[9] See GAO, *DOD Critical Technologies*, GAO-21-158 (Washington, DC: Government Printing Office, 2021), pp. 2-3; UK Ministry of Defence, *National Security Through Technology*, CM 8278 (London: The Stationary Office, 2021), 2.4.

[10] See Christopher A. Bidwell and Bruce W. Macdonald, *Emerging Disruptive Technologies and Their Potential Threat to Strategic Stability and National Security* (Federation of American Scientists, 2018): p. 17-18 and 28.

[11] See NATO, *Foster and Protect: NATO's Coherent Implementation Strategy on Emerging and Disruptive Technologies*, 15 July 2022, at: https://www.nato.int/cps/en/natohq/topics_184303.htm

data analytics far beyond the capabilities of today's supercomputers. Quantum communications and encryption technologies promise an impenetrable computer network protected by quantum encryption guaranteeing the safe transmission of data in real time and preventing the spoofing, corruption, or interception of communications.[12] Quantum encryption will also permit access to all non-quantum encrypted networks and data. In the post-quantum world, military communications will have a binary character: secured or unsecured. Lastly, quantum sensors embedded in satellite mesh networks will enable comprehensive maritime situational awareness, the detection of the currently invulnerable submarine component of national nuclear deterrents, and a terrestrial substitute for vulnerable space-based positioning, navigation, and timing systems (PNT).[13]

> *"Developments in AI, quantum, hypersonic, and directed energy weapons technologies will inevitably shift the offensive-defensive balance in ways that will aggravate the security dilemma. The inevitable shift to an offensive strategy is problematic for a self-declared defensive alliance, especially since NATO derived and sustained its political legitimacy from that mission."*

Lethal Autonomous Weapons Systems

LAWS are capable of selecting and engaging targets independent of human agency. The deadly dynamic of LAWS—the maximum advantage of deploying LAWS will accrue to those who place humans from the "kill chain" at the furthest remove—offers a first-mover advantage compounded by the absence of an operational distinction between offensive and defensive capability or intent. These characteristics promise to exacerbate the security dilemma in all war-fighting domains, conventional or nuclear.[14] The trans-domain proliferation of LAWS has produced a range of weapons systems collectively known as UxVs. The most consequential include unmanned air vehicles (UAV for ISR or UCAV if armed) and unmanned surface or submarine maritime vessels (USV and UUV, respectively).[15] Maritime LAWS will enhance

[12] Michiel van Amerongen, *Quantum Technologies in defense & security* (NATO Review,2021): p. 5-6.

[13] See Jacopo Bellasio and Erik Silfersten, *The Impact of New and Emerging Technologies on the Cyber Threat Landscape and Their Implications for NATO*, (Tallinn: CCDCOE, 2020): p. 96.

[14] Jürgen Altman and Frank Sauer, *Autonomous Weapons Systems and Strategic Stability* (Survival, Vol. 59, No. 5, 2017): p. 119-21.

[15] NATO STO, *2020 Highlights: Empowering the Alliance's Technological Edge,2020-2040* (Brussels: NATO STO, 2020a): p. 60, www.sto.nato.int

the effectiveness of mine-countermeasure and anti-submarine warfare.[16] Aerospace LAWS will enable swarm technologies for the purposes of theatre ISR missions and potentially for neutralizing enemy A2/AD forces or enhancing one's own.[17] Space-based UxV applications currently lack kinetic capabilities, but directed energy weapons technologies could disable maritime and aerospace UxVs that depend upon secure access to the space commons. Aerospace and maritime LAWS also possess two terrestrial advantages: they minimize casualties and reduce personnel requirements, important force multipliers for NATO owing to the public aversion to casualties and unfavorable long-term demographic trends.[18]

Hypersonic Technologies

Hypersonic boost-glide and cruise missiles, which exceed Mach 5 and have low trajectories, can evade existing anti-missile ballistic defense systems. Both Russia and China have deployed hypersonic missiles to NATO's dismay: it constitutes "proof" that NATO has lost its technological edge and now places NATO forces at a tactical and strategic disadvantage.[19] Maneuverable hypersonic degrade strategic stability by introducing endemic ambiguity with respect to warhead and target, but the kinetic energy released by a hypersonic missile without a warhead makes possible a counter-force nuclear war-fighting strategy with violating the nuclear threshold.[20] Finally, hypersonic weapons-augmented A2/AD strategies will expand the defensive maritime periphery of continental powers and reduce the maritime advantage NATO currently enjoys. A hypersonic missile interceptor system would alleviate these threats to NATO operational dominance but detecting and tracking hypersonic missiles depends upon secure space-based infrared sensors—something that cannot be guaranteed.[21]

Space Technologies

Space is the "high ground" of any future great power conflict and the NATO states are, compared to Russia and China, asymmetrically dependent upon space-based

[16] Bundesministerium der Verteidigung, *Wehrwissenschaftliche Forschung Jahresbericht 2020* (Berlin: BMVg, 2020): p. 92-93.

[17] NATO STO (2020a): p. 60.

[18] O'Rourke, Ronald, *Navy Large Unmanned Surface and Undersea Vehicles*, R45757 (Washington, DC: CRS, 2022), p. 1.

[19] NATO STO, *Science & Technology Trends 2020-2040: Exploring the S&T Edge* (Brussels: NATO STO, 2020b),pp. 89-91; UK, Secretary of State for Defence, *Defence in a competitive age*, CP 411 (London: The Stationary Office, 2021), §2.2.

[20] Fabio Rugge, "The Global Race for Technological Superiority" in *idem.* (ed.), *The Global Race for Technological Superiority* (Milan: ISPI, 2019), pp. 32ff.

[21] Raytheon, "Missile Defense Agency selects Raytheon Missiles & Defense to develop first-ever counter-hypersonic interceptor**,"** *Raytheon Technologies*,19 November 2021, https://www.rtx.com/News/News-Center/2021/11/19/missile-defense-agency-selects-raytheon-missiles-defense-to-develop-first-ever

assets. NATO space dominance is double-edged: the exploitation of space has lent NATO a battlefield advantage on land and sea and in the air, but dependence upon space-based assets for ISR, PNT, command and control, UxV operations, and communications represents a source of vulnerability as space transitions from an enabling, militarized domain to a weaponized battle space.[22] The range of offensive technologies capable of blinding or disabling space-dependent weapons platforms range from direct-assent weapons to directed energy weapons to electromagnetic pulse weapons, among others.[23] They collectively pose a direct threat to the effectiveness of NATO military operations in the event of great power war. A deterrence strategy is unlikely to alter that vulnerability: Russian and Chinese forces are much less dependent on space-based assets for operational effectiveness. Nonetheless, there are mitigating technologies on offer: interference with ISR will be limited once quantum encryption is fully developed just as free space optical communication technologies will limit the interception of satellite-to-satellite communications. FSO augmented satellites will be less expensive than current communications satellites, enabling greater redundancy in an integrated satellite mesh network, and they present a much smaller target than current satellites, reducing the risks of either a ballistic missile and high-energy assault.

Artificial Intelligence (AI)

Most observers view AI as the critical defense technology of the future. The NATO Science & Technology Organization endorsed Christopher Bidwell and Bruce Macdonald's claim that AI "is going to be the biggest geopolitical revolution in history."[24] These claims depend upon the successful transition from artificial narrow intelligence (the current state of AI technologies) to artificial general intelligence—a remote eventuality at best. But AI carries some liabilities: it may well be vulnerable to data poisoning, flawed algorithms, or AI-generated disinformation.[25] The fusion of AI and quantum computing technologies will enhance ISR capabilities, foster trust and enhance the effectiveness of LAWS, and provide a data analytics advantage for the country or alliance that does so first. Yet the postulated first-mover advantage accruing to NATO (or China) with respect to AI will likely be short-lived—the private sector constitutes the leading-edge in AI research and the profit motive all but guarantees that AI and big data will be commodified at the expense of national security.

[22] See Beyza Unal, *Cybersecurity of NATO's Space-based Strategic Assets* (London: Chatham House, 2019), pp. 9-16; and NATO, *NATO's overarching Space Policy*, 17 January 2022, https://www.nato.int/cps/en/natohq/official_texts_190862.htm?utm_source=linkedin&utm_medium=nato&utm_campaign=20220117_space

[23] See Brian Weeden and Victoria Samson, *Global Counterspace Capabilities* (Washington, DC: Secure World Foundation, 2019): p. 7.1-7.9.

[24] See NATO STO (2020b): p. 53.

[25] See Mark Fitzpatrick, *Artificial Intelligence and Nuclear Command and Control* (Survival, Vol. 61, No. 3, 2019): p. 91.

Potential Strategic Consequences of EDTs

EDTs will have first, second and third order consequences for NATO. The first order effects occur when technological innovations alter the offensive-defensive balance or the nature of war-fighting within a single domain; second order effects occur when the technological change induces a shift in the offensive-defensive balance across war-fighting domains; and third order effects occur when a suite of EDTs narrow or invert existing power differentials among polar powers or give rise to new ones. The EDTs identified in NATO documents as well as those of the major NATO states are generally cross-cutting in terms of application and effect, a phenomenon reinforced with the advent of multi-domain warfare—itself a product of these EDTs and the U.S. Department of Defense aspiration to achieve total battlefield situational awareness and the concept of joint domain warfare initiated with the Goldwater-Nichols Reorganization Act.[26]

Anti-satellite and hypersonic EDTs will have specific war-fighting-domain consequences. Anti-satellite technologies pose a kinetic threat (as distinct from cyber- or electronic warfare) to a range of capabilities, not the least among them being the NATO member-state PNT satellite systems (the American GPS, the European Galileo, and the French DORIS).[27] As noted above, these counter-force technologies have weaponized space and increased the ease with which adversaries can disrupt or destroy vital space assets. Hypersonic weapons are also candidates for altering the nature of maritime warfare. In the absence of a dependable anti-ballistic missile defense capability, hypersonic missiles have the potential to alter warfare akin to the replacement of Dreadnaughts by aircraft carriers in the mid-20th century. The postulated inability to protect carriers from this new weapons category—especially as the technology becomes diffused throughout the international system—will multiply the number of adversaries that can effectively thwart NATO's current strategic advantage derived from carrier-based force projection.[28]

Developments in AI, quantum, hypersonic, and directed energy weapons technologies will inevitably shift the offensive-defensive balance in ways that will aggravate the security dilemma. The inevitable shift to an offensive strategy is problematic for a self-declared defensive alliance, especially since NATO derived and sustained its political legitimacy from that mission. The integration of these technologies into

[26] See David A. Deptula, *A New Battle Command Architecture for Joint All-Domain Warfare* (*ÆTHER: A Journal of Strategic Airpower & Spacepower,* Vol. 1, No. 1 2022): p. 52.

[27] Defense Intelligence Agency, *Challenges to Security in Space: space reliance in an era of competition and expansion* (Washington, DC: DIA, 2022): p. 9-10.

[28] See O'Rourke (2022): p. 39-41; and Colin Meyer, *The Navy's Big Carrier Groups are Sitting Ducks* (Wall Street Journal, 14 April 2022).

future weapons platforms will call into question that mission despite best efforts to maintain fidelity in rhetoric and doctrine to collective defense; NATO doctrine will inevitably acquire an offensive character despite an embedded aversion to it. NATO will become a more lethal and threatening adversary, but their inherent offensive character may disrupt the strategic status quo in such a way that it erodes the alliance's legitimacy with a substantial share of the left-leaning, reflexively pacifist European. Although quantum encryption and free space optical communications are inherently defensive in nature, that very characteristic will force decision-makers to adopt worse case assumptions about their adversaries: the future inability to penetrate an adversary's information networks will defeat efforts to acquire signals intelligence that provide antagonists to formulate a more realistic assessment of an adversary's capabilities and intentions. AI is the most destabilizing technology if its promise is realized and integrated into LAWS. Those states relying upon (dependable) AI will be able to engage in warfare at a lower political cost (in terms of human casualties) and do so with lower manpower requirements that currently consume up to 50 percent of NATO member-state defense budgets, thereby freeing funds to purchase those AI-dependent weapons systems and reinforce a reliance upon them.[29] AI encodes a deadly logic: on an AI-dominated battlefield, the state willing to remove humans fully from the "kill-chain" will enjoy a lethal advantage vis-à-vis states that insist on ensuring that humans remain in it. The logic of AI forces every state to place humans at the same link in the "kill chain". The state placing humans at the furthest remove—the absence of human agency—will achieve a strategic and tactical advantage to any adversary not doing so. This dynamic poses internal and external challenges for NATO. There is not only no common global approach to AI-augmented weapons, but NATO itself presently "lacks a common approach to governance and the use of AI, autonomy and automation…"[30] It is also highly unlikely that an intra-alliance consensus can be reached on the outer limits of autonomy from human interference, an absence that could easily generate technologically caveated armed forces and create willy-nilly an operationally bifurcated alliance limiting the effective aggregation of NATO capabilities.

If these technologies are as critical as alleged to maintaining NATO's technological edge vis-à-vis potential adversaries, then it is also a near certainty that NATO's adversaries will seek the same. This dynamic virtually ensures that the NATO edge will be narrowed sooner than later. There are already certain sub-fields of AI and quantum technologies where the Chinese are assumed to have a lead over the U.S. and other NATO states in terms of development, although the translation of that technological advantage into a military advantage remains ambiguous presently. It

[29] See European Parliamentary Research Service, *Innovative technologies shaping the 2040 battlefield* (Brussels: EPRS, 2021): p. 22.

[30] See NATO ACT (2020).

is incontrovertible, however, that Russia and China have a deployed capability—hypersonic missiles—that may make obsolete critical pillars of NATO force projection capabilities and, perhaps more important, reduce the credibility of the American security guarantee. It is a near certainty that quantum technologies and AI will be quickly diffused throughout the international system—the profit motive of the leading-edge corporations developing these technologies will override any concern with national security. As a consequence, these EDTs will inevitably produce a narrowing of the power differential between the NATO states and China, particularly. But it is less likely that the current technological edge enjoyed by NATO will be erased or that there will be a tectonic rather than evolutionary reordering of the global balance of power, the end point of which remains indeterminate.

Conclusion: NATO Cohesion and EDTs

There are any number of disruptive impacts that EDTs may have on intra-alliance cohesion. The most significant internal challenges to NATO cohesion and operational effectiveness can be traced to the necessity of balancing the costs and benefits of technology sharing and technology hoarding among allies, particularly where it touches upon ISR; the barrier to interoperability caused by the integration of those technologies into weapons systems that will put them out of the financial reach for all but the largest NATO member states; and the prospect of nuclear deterrence based on counter-value retaliation displaced by counterforce war-fighting once quantum gravity sensors are developed—a technological innovation that will make the 24/7 tracking of heretofore invulnerable ballistic missile submarines possible. These challenges are aggravated by the European concern that they are overly dependent upon U.S. technology and should implement policies targeting the reclamation of technological sovereignty, particularly as it pertains to cryptology and cyberspace,[31] by the inevitable American complaints about burden-sharing if resources are devoted to European autonomy rather than measures supporting American dominance and dependence, and by disagreements on how to respond to the continued depredations of revisionist powers that have closed the technology gap with the West. Each of these potential technology-driven developments could significantly strain allied cohesion and effectiveness.

Despite the anticipated disruptions caused by these technologies, it is tempting to remain sanguine about their external and internal consequences for NATO. In the post-war past, analysts viewed contemporaneous technological changes as revolutionary and as harbingers of tectonic shifts in battlefield advantage, power

[31] See NATO STO (2020b): p. 47-48; Bundesministerium der Verteidigung (2020): p. 154-55. See also, Paula Forteza, Jean-Paul Herteman, Iordanis Kerenidis, *Quantitque:le virage technologique que la France ne ratera pas* (Paris: 2019), at: https://forteza.fr/wp-content/uploads/2020/01/A5_Rapport-quantique-public-BD.pdf

differentials, or global hegemony. In retrospect, those past shifts appear to have been closer to the evolutionary rather than revolutionary end of the spectrum. Yet, it seems likely that this cycle of technological innovation will be as disruptive as were the introductions of gunpowder and nuclear weapons. These technologies will yield untoward shifts in the offensive-defensive balance and the squeezing of power differentials to NATO's disadvantage; it will yield a geopolitical and geostrategic constellation of power that will jeopardize the West's ability to protect the existing rules-based international order. Unlike the past, these new technologies will have the perverse effect of narrowing the technological gap between NATO and the rest, while exacerbating the existing technological and interoperability gaps within the alliance.