Routledge
Taylor & Francis Group

Whitehall Papers

ISSN: 0268-1307 (Print) 1754-5382 (Online) Journal homepage: https://www.tandfonline.com/loi/rwhi20

VIII. Maintaining NATO's Technological Edge

Tim Sweijs & Frans Osinga

To cite this article: Tim Sweijs & Frans Osinga (2019) VIII. Maintaining NATO's Technological Edge, Whitehall Papers, 95:1, 104-118, DOI: 10.1080/02681307.2019.1731216

To link to this article: https://doi.org/10.1080/02681307.2019.1731216

Published online: 04 Apr 2020.

VIII. MAINTAINING NATO'S TECHNOLOGICAL EDGE

TIM SWEIJS AND FRANS OSINGA

The character of modern armed conflict is changing rapidly. Major powers have integrated new generations of military hardware as well as an assortment of enabling technologies into their force postures and warfighting strategies. Violent non-state actors have also significantly enhanced their power projection capabilities. These developments have a profound impact on the conditions underlying international stability and will change the face of battle. This chapter first outlines current and near-future (five- to 10-year) developments in cyber, artificial intelligence (AI), unmanned systems and space, and assesses their consequences for international security and stability. It then examines the implications for NATO, arguing that the Alliance risks losing its military-technological edge vis-à-vis near-peer competitors if it does not increase its investments and efforts in these areas. It also lays out the strategic, moral and practical challenges that these new technologies pose, in particular for European member states, and offers four recommendations for NATO action going forward.

Military-Technological Trends and their Military-Strategic Implications

Cyber

Cyberspace has now been established as another warfighting domain and strategists have moved beyond debating whether or not cyber war will take place.[1] The past decade saw countries develop cyber weapons and doctrines and establish cyber commands to execute operations in the

[1] Thomas Rid, 'Cyber War Will Not Take Place', *Journal of Strategic Studies* (Vol. 35, No. 1, 2012), pp. 5–32.

cyber domain. This early phase in cyber warfare also featured the first deployment of cyber instruments in the context of military operations alongside continuous lower-level cyber skirmishes, infiltrations of adversary networks, large-scale theft of critical national security technologies and sabotage of vital infrastructures.[2] In the next phase, states will continue to expand and refine their cyber arsenals and experiment with cyber operations to explore the extent to which they can achieve operationally and strategically relevant effects. Both theory and practice regarding the use and utility of cyber weapons as strategic instruments will gain more depth and breadth in continuous and close interaction with each other. If initial state military cyber forays could be characterised, in one of Deng Xiaoping's unforgettable phrases, as 'crossing the river by feeling the stones', the next few years are likely to involve greater experimentation, followed, eventually, by some degree of maturation, analogous to the way air strategy and doctrine developed in the first half of the 20th century.

The still-nascent strategic knowledge base concerning how military cyber weapons can be created, maintained and used will inevitably expand and spread to more state and non-state actors. It will include best practices and standard procedures for how to structure 'exploit development cycles', how to compare and rate the strategic value of classes of zero-day vulnerabilities and when to best make use of them given their 'transitory nature'.[3] This will undoubtedly result in a more differentiated and mature portfolio of cyber weapons. Meanwhile, both military and political decision-makers will likely improve their understanding of the cyber domain and the potential effects of cyber weapons. This will be facilitated by the further elaboration and refinement of strategies and doctrines describing when and how cyber instruments can be deployed.

At the operational level, cyber capabilities will be critical enablers of military action. Even more than now, the conduct of future war will depend on command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) capabilities. Robust cyber network protection will therefore be a sine qua non for any future fighting force. Offensive military cyber capabilities will be instrumental in blinding

[2] Alexander Klimburg, *The Darkening Web: The War for Cyberspace* (New York, NY: Penguin Press, 2017).

[3] Lillian Ablon and Andy Bogart, *Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits* (Santa Monica, CA: RAND Corporation, 2017), pp. 65–72; Max Smeets, 'A Matter of Time: On the Transitory Nature of Cyberweapons', *Journal of Strategic Studies* (Vol. 41, No. 1–2, 2018), pp. 6–32.

the enemy by eliminating adversarial C4ISR structures. At the tactical level, power will be partially pushed to the edge, with capabilities trickling down to tactical cyber units that will have access to reach-back facilities. This will occur in the context of the further fusion of the cyber and electromagnetic spheres, leading to the formation of cyber and electromagnetic activities (CEMA) teams.

Meanwhile, continued progress in AI will further drive the automation of both offensive and defensive cyber tasks (for example, identifying critical vulnerabilities in adversary systems or patching security gaps). This will expedite the development of 'cyber centaur' squads consisting of smart cyber programmers working in close synergy with even smarter algorithms, with the latter performing most of the complex work. Despite Google's recent claim that it has attained the 'quantum supremacy' milestone, the level of progress in quantum computing is not expected to make encryption obsolete and usher in a world of full transparency during the next decade.[4]

Over the next five years, the arrival of 5G networks will bring about the Internet of Everything, multiplying opportunities to create chaos and wreak havoc on our societies. This will facilitate two parallel developments, both of which have already started. First, it will drive the nationalisation of control over critical infrastructures and the subsequent fragmentation of the global internet. Second, it will motivate state and non-state actors to further embrace offensive cyber doctrines so that they can significantly threaten not just the military capabilities of their opponents but, and potentially more effectively from a strategic perspective, their entire societies through attacks on critical infrastructures. The exploitation of social media for the targeted distribution of disinformation will undermine societal trust in Western democratic states. Russia's intrusions into Ukrainian and US critical national infrastructures, as well as the centrality of concepts such as persistent engagement in 'grey space' and 'red space' in recent high-level US debates on cyber operations, may in that respect be only early harbingers of what is to come.[5]

[4] Michael E O'Hanlon, 'Forecasting Change in Military Technology, 2020–2040', Brookings Institution, September 2018.

[5] In the US Joint Publication 3-12 on cyberspace operations, 'blue space' refers to areas in cyberspace protected by the US, 'red space' refers to cyberspace owned or controlled by an adversary and 'grey space' refers to 'all cyberspace that does not meet the description of either "blue" or "red"'. See US Department of Defense, 'Joint Publication 3-12: Cyberspace Operations', 8 June 2018, p. I-5.

Artificial Intelligence

AI is an all-purpose enabler that will profoundly shape the ways in which armed forces fight, similar to how the internal combustion engine and the computer changed the conduct of war in previous eras.[6] The past decade saw considerable progress in deep learning and neural networking, commonly captured under the rubric of AI. During this period, machine-learning applications revolutionised a wide range of activities, from Wall Street trading (with algorithms executing over 40% of the trades) and advertising (micro-profiling and behavioural targeting), to health sciences (cancer screening). In the past two years, major military powers, in particular the US and China, have expanded their investments, with Russia, Israel, France and the UK following at a distance. Things are moving fast now: military powers publish AI strategies and establish well-funded AI centres at the heart of military institutions. Countries actively pursue civil–military fusion; in particular, China's People's Liberation Army (PLA) seeks to harness and exploit private and civil innovation through institutionalised cooperation. Current AI applications include early warning (predictive modelling), intelligence analysis (signal detection), battlespace and course-of-action analysis, target acquisition and recognition, swarming manoeuvre techniques, and command and control (C2) and (semi-)autonomous decision-making. In this context, the Chinese speak of 'intelligentized warfare', with reference to the US notion of informatised war of the 1990s when the Second Offset Strategy of the 1970s started bearing fruit.[7]

A dystopian future in which machines are not only involved in the conduct of operations but also make the decisions – which would, in effect, change the nature of war – is still a long way off.[8] The character of war will change, however, as a result of the progressive integration of AI in the modus operandi of armed forces over the course of the 2020s. Incremental improvements to military capabilities will likely ensue after a period of trial and error, and will likely also lead to benefits that include greater safety of combatants and non-combatants. A fundamental concern, however, relates to whether the successful integration and exploitation of future generations of AI will yield a quantum capability leap that will then

[6] Michael C Horowitz, 'Artificial Intelligence, International Competition, and the Balance of Power', *Texas National Security Review* (Vol. 1, No. 3, May 2018), pp. 36–57.

[7] Elsa B Kania, 'Battlefield Singularity: Artificial Intelligence, Military Revolution, and China's Future Military Power', Center for a New American Security, 28 November 2017, p. 12.

[8] F G Hoffman, 'Will War's Nature Change in the Seventh Military Revolution?', *Parameters* (Vol. 47, No. 4, Winter 2017–18), pp. 19–31.

dramatically upset the military balance of power. Such punctuated progress may translate into first-past-the-post advantages for early adopters. Historical military parallels exist: in the past, Western powers attained a decisive military edge that lasted several centuries when they first exploited the gunpowder revolution and then unleashed the power of the Industrial Revolution in the service of military objectives. The exact form military superiority will take in the 'age of AI' is not yet clear, but military strategists on all sides are obviously hastening to envision and engineer the force of the future. Likely consequences in this time period associated with military AI applications include the cumulative acceleration of the OODA (observe, orient, decide, act) loop, the partial removal of humans from some aspects of this loop and the advent of 'hyperwar' through the employment of AI-equipped autonomous weapon systems.[9]

Unmanned Systems

Closely related to progress in computing power and smarter algorithms is the proliferation of unmanned platforms in the land, sea and air domains. Over 150 types of military aerial drones are in production in nearly 50 states, more than 100 states deploy drones for military purposes and at least 36 states possess, or are in the process of acquiring, armed drones.[10] At present, these drones are used primarily for C4ISR and strike. In recent years, Western powers, relying on air superiority, exploited their lead in military drone capabilities to wage a form of remote warfare: they targeted insurgent and terrorist groups, and in January 2020 even a key Iranian general, while themselves remaining seemingly invulnerable to counter-strike.[11] But the proliferation of drones will certainly put this presumed invulnerability under pressure. Due to low costs and easy availability, both state and non-state actors are obtaining and employing drones. A September 2019 article in the *New York Times*, headlined 'Boko Haram is Back. With Better Drones', captures a much wider trend prevailing in battle theatres around the globe. The Islamic State of Iraq and Syria (ISIS) has carried out attacks against Syrian civilians and Russian bases, Hizbullah has deployed them in Syria and Venezuelan opposition forces

[9] Paul Scharre, *Army of None: Autonomous Weapons and the Future of War*, first edition (New York, NY: W W Norton & Company, 2018).

[10] Center for a New American Security, 'Proliferated Drones: The Drone Database', <http://drones.cnas.org/drones/>, accessed 5 November 2019; New America, 'Who Has What: Countries with Armed Drones', <https://www.newamerica.org/in-depth/world-of-drones/3-who-has-what-countries-armed-drones/>, accessed 5 November 2019.

[11] Andreas Krieg and Jean-Marc Rickli, 'Surrogate Warfare: The Art of War in the 21st Century?', *Defence Studies* (Vol. 18, No. 2, 2018), pp. 113–30.

used a drone in an attempt to assassinate President Nicolás Maduro. Libyan armed groups also employed Chinese- and Turkish-manufactured drones in the ongoing civil war in summer 2019.

Progress in unmanned land and maritime vehicles has lagged somewhat behind advances in aerial platforms, but Russia, which aspires to make 30% of its land systems robotic by 2025, has already tested the Uran-9 tank in Syria. In 2018, President Vladimir Putin announced that Russia was developing the autonomous, intercontinental-range, nuclear-powered unmanned underwater vehicle (UUV), Poseidon, to carry out nuclear attacks. China displayed a revolutionary UUV alongside an air-launched supersonic drone at its 70th National Parade on 1 October 2019 and has launched an expansive programme involving the domestic production of a variety of unmanned systems for land and naval warfare.[12] As yet another sign of China's rise, it recently overtook the US as the world's foremost exporter of drones.

Trends in this sphere point towards the further proliferation of unmanned systems featuring miniaturisation and far greater endurance. Such systems will further fuel the ongoing expansion of violence and contribute to levelling the playing field between technologically advanced and less advanced actors. As T X Hammes observes, 'the proliferation of many small and smart weapons may simply overwhelm a few exceptionally capable and complex systems'.[13]

Space

Space assets are increasingly central to the functioning of globally networked societies. Satellite launch capabilities are proliferating, while the cost of satellites is decreasing. Fourteen states can now launch their own satellites and more than 80 states possess space-based assets, while numerous commercial providers offer services from space to anyone who can afford them.[14] Space-based assets are also increasingly critical enablers of current and future military operations, with most CS4IR functions depending on them. Major military powers without space-based assets are in essence deaf, blind and mute, and indeed paralysed.

[12] Vincent Boulanin and Maaike Verbruggen, 'Mapping the Development of Autonomy in Weapon Systems', SIPRI, November 2017, pp. 102–03; Office of the US Secretary of Defense, 'Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2019', May 2019.

[13] T X Hammes, 'Technologies Converge and Power Diffuses: The Evolution of Small, Smart, and Cheap Weapons', Cato Institute, Policy Analysis No. 786, 27 January 2016.

[14] Linda Dawson, *War in Space: The Science and Technology Behind Our Next Theater of Conflict* (New York, NY: Springer International Publishing, 2018), p. 13.

Intelligence, communication, precision weapons and logistics all depend on properly functioning space systems.

Not surprisingly, space is increasingly regarded as a military domain. Space is now starting to be weaponised, the terms of the 1967 Outer Space Treaty notwithstanding. In March 2019, India became the fourth country to demonstrate a direct-ascent anti-satellite (ASAT) capability in a live test, following the US, Russia and China, which first did so in 2007. These tests are emblematic of a more pervasive trend. The US, under President Donald Trump, re-established a Space Command in 2019 as a precursor to an eventual Space Force. In China, the Strategic Support Force, established in 2015, has an important role in further developing the PLA's space warfare capabilities. Russia, building on the vast infrastructure established during Soviet times, remains an important space power.

In strictly military terms, Europe's space powers lag behind China, Russia and the US, which are currently recalibrating their military space postures and are actively investing not only in greater numbers of satellites, but also in stronger protection of those systems, better encrypted download and upload datalinks, and further development of ASAT missile systems, satellite jammers and directed energy weapons.[15] China has embarked on a manned programme seeking to establish a research station on the Moon in the mid-2020s and to post humans there for extended periods in the 2030s.[16] The US also intends to return to the Moon; the first unmanned mission to transport cargo is planned for 2021, to be followed by a manned mission in 2024.[17]

Meanwhile, billionaires Elon Musk, Jeff Bezos and Richard Branson have each launched their own space corporations, based on grand visions of space exploration, exploitation and colonisation. At the same time, the US government is redrafting its rules and regulations, no longer designating space as a 'global commons' but clearly pursuing the objective to 'unshackle business activity in space'.[18] If history is any guide, attempts to establish control over economic resources will likely be accompanied by the deployment of military power to enforce and

[15] US Defense Intelligence Agency, 'Challenges to Security in Space', January 2019, pp. 23–28; National Air and Space Intelligence Center, 'Competing in Space', December 2018.

[16] Steven Lee Myers and Zoe Mou, '"New Chapter" in Space Exploration as China Reaches Far Side of the Moon', *New York Times*, 2 January 2019.

[17] Kenneth Chang, 'Why Everyone Wants to Go Back to the Moon', *New York Times*, 12 July 2019.

[18] Victor L Shammas and Tomas B Holen, 'One Giant Leap for Capitalistkind: Private Enterprise in Outer Space', Palgrave Communications (Vol. 5, No. 10, 2019); US Department of Commerce, 'Secretary Ross: "A Bright Future for U.S. Leadership of Space Commerce"', 21 February 2018.

guarantee that control. Space, in sum, truly constitutes a new frontier for the conduct of terrestrial and, down the line, extra-terrestrial competition and conflict.

Implications for NATO

The literature on revolutions in military affairs (RMAs) suggests that those who manage to harness and exploit new technologies, combine them with novel operational and organisational concepts and evolve a new way of war stand to gain significantly – a sobering insight in this era of strategic competition. This is not lost on, for instance, Putin, who highlighted the impact of AI on the international order when he observed that 'artificial intelligence is the future, … whoever becomes the leader in this sphere will become the ruler of the world'.[19] Chinese leaders have expressed similar views.[20]

Whether the technological trends described above signal the advent of another RMA or merely represent incremental change remains subject to debate.[21] Regardless, the implications of the technological progress summarised here are already being made manifest and are likely to progressively materialise during the 2020s. The first attacks with swarms of drones have already taken place in Syria, Libya and Saudi Arabia, executed not by a state but by various non-state actors.

NATO members already face an assortment of challenges, including the vicious conflict dynamics in Northern Africa, the Middle East and Southwest Asia, which are not likely to disappear soon. Further, Russia's nuclear and conventional modernisation, in combination with its anti-access/area denial (A2/AD) capabilities, has cast doubt on the credibility of NATO's conventional and nuclear deterrence posture.[22] In this latter context, it has become painfully clear that the armed forces of European NATO members, in particular, have neglected the demands of joint high-intensity warfare at their own peril. For NATO, these developments therefore suggest, at a minimum, a strong imperative to not only rebuild its capabilities, but also to keep pace with rapid technological advances.

---

[19] James Vincent, 'Putin Says the Nation That Leads in AI "Will Be the Ruler of the World"', *The Verge*, 4 September 2017, <https://www.theverge.com/2017/9/4/16251226/russia-ai-putin-rule-the-world>, accessed 7 February 2020.

[20] As quoted in the read-ahead package for the NATO-Industry Forum, Berlin, 12–13 November 2018, p. 10.

[21] Kenneth Payne, *Strategy, Evolution, and War: From Apes to Artificial Intelligence* (Washington, DC: Georgetown University Press, 2018); Christian Brose, 'The New Revolution in Military Affairs: War's Sci-Fi Future', *Foreign Affairs*, May/June 2019.

[22] Elbridge Colby and Jonathan Solomon, 'Facing Russia: Conventional Defence and Deterrence in Europe', *Survival* (Vol. 57, No. 6, November 2015), pp. 21–50.

NATO Initiatives

In recent years, NATO launched a series of initiatives to regain capabilities and expertise, with member states pledging to increase defence spending. Current capability improvement plans focus on enhancing readiness, regaining lost capabilities in artillery, tanks, transport and C2 assets; and introducing fifth-generation jet fighters in greater numbers than those ordered prior to 2014. Cyber capabilities are also receiving a boost now that cyberspace has been designated a warfighting domain. The Alliance will enhance missile defence in the next decade by fielding state-of-the-art US radar systems in various Eastern European member states. Furthermore, NATO has formulated a roadmap for research on emerging technologies such as AI, quantum computing, autonomy and hypersonic missiles. Various organisations, such as NATO's Science and Technology Organization (STO) and different centres of excellence, aim to support knowledge diffusion, create awareness and stimulate research and development. The STO conducts research on more than 250 projects across seven domains that canvass a wide spectrum of emerging technologies.[23]

European NATO member states that are also EU members have similarly agreed on a series of capability improvement initiatives. Following the 2016 EU Global Strategy, the EU launched the Coordinated Annual Review on Defence (CARD), the Permanent Structured Cooperation (PESCO) and the European Defence Fund (EDF). These initiatives focus on the range of capability targets identified in the 2018 update to the EU Capability Development Plan. The goals are to achieve a measure of strategic autonomy and to create a coherent full-spectrum force package. This force package aims to ensure air and information superiority and access to space-based systems; to support cyber response operations, naval manoeuvrability and air mobility; and finally, and more generically, to develop 'innovative technologies for enhanced future military capabilities'.[24] The US, meanwhile, has announced its determination to leverage the potential of emerging technologies in what has been labelled the 'Third Offset'. In parallel with this initiative, the US is exploring a new operational concept – 'Multi-Domain Operations' – that harnesses and exploits these new capabilities and may play the same role as the AirLand Battle concept of the 1980s.[25]

[23] See NATO Science and Technology Organization, 'Empowering the Alliance's Technological Edge: 2018 Highlights', March 2019, <https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_09/20190905_190905-STO-highlights2018.pdf>, accessed 7 February 2020.

[24] European Defence Agency, 'The EU Capability Development Priorities', 2018, pp. 6–7.

[25] David G Perkins and James M Holmes, 'Multidomain Battle: Converging Concepts Toward a Joint Solution', *Joint Force Quarterly* (Vol. 88, January 2018), pp. 54–57.

Challenges

Despite these efforts, the developments sketched in this chapter present NATO members with an assortment of financial, ethical and military-strategic challenges. For NATO's European member states in particular, the Third Offset poses a considerable financial burden.[26] Although European member states currently spend $264 billion collectively on defence, and despite a decade of improvement initiatives, the capability shortfalls that came to light in Operation *Allied Force* in Kosovo in 1999 persist.[27] In 2012, one study concluded that without US contributions, Europe would struggle to conduct a so-called 'Small Joint Operation, Air-Heavy' – an operation comparable to Operation *Allied Force* or *Unified Protector* in Libya (2011).[28] In 2020, European armed forces remain critically dependent on the US for C4ISR and suppression of enemy air defences (SEAD) capabilities, cruise missiles, ballistic missile defence, stealth aircraft and electronic warfare assets. The same applies to creating and manning effective operational headquarters that rely on state-of-the-art C2 technology as well as expertise in operational-level planning and commanding joint operations. Estimates indicate that without the US, the defence of the Baltic states and Poland would require an additional investment by European states of about $288–357 billion.[29]

Adapting to the new geopolitical environment and implementing capability improvements for their armed forces has proven difficult for Europe's defence organisations, however, not least because of budgetary realities.[30] Defence cooperation initiatives also suffer because European defence industries remain fractured and compartmentalised along national lines, and have a diminishing ability to nationally develop and manufacture complex leading-edge military capabilities. Remedying several of the capability shortfalls – those pertaining to large and complex systems such as tanker aircraft or electronic warfare platforms – also exceeds the requirements of individual countries and calls for collective action. In addition, actually fielding the necessary new capabilities takes at least a decade.[31] Finally, while high-end weapon systems and emerging

[26] Luis Simón, 'The "Third" US Offset Strategy and Europe's "Anti-Access" Challenge', *Journal of Strategic Studies* (Vol. 39, No. 3, 2016), pp. 417–45.
[27] Douglas Barrie et al., 'Defending Europe: Scenario-Based Capability Requirements for NATO's European Members', International Institute for Strategic Studies, April 2019, p. 3.
[28] F Stephen Larrabee et al., *NATO and the Challenges of Austerity* (Santa Monica, CA: RAND Corporation, 2012), p. ix.
[29] Barrie et al., 'Defending Europe'.
[30] Jens Ringsmose and Sten Rynning, 'Now for the Hard Part: NATO's Strategic Adaptation to Russia', *Survival* (Vol. 59, No. 3, 2017), pp. 129–46.
[31] Barrie et al., 'Defending Europe', p. 42.

technologies claim much of the Alliance's attention, funds will also be needed for restoring more mundane capabilities such as ammunition stockpiles and transport capacity, which will enable rapid reinforcement and a sustained military campaign. Given the rather dismal European track record in actually achieving military transformation as envisioned by NATO, investments in Third Offset technologies may never actually materialise and might not produce the necessary improvements even if they did.[32]

Another challenge lies in the controversial nature of some of these technologies. While the technologies may yield many military benefits, the legality and ethics of, for instance, deploying unmanned and semi-autonomous weapon systems are hotly debated throughout society, academia, parliaments and religious circles (including the Vatican). Expert groups discuss the ethical and legal issues associated with military AI, including in the context of the UN Convention on Certain Conventional Weapons. António Guterres, former UN Secretary-General, captured prevailing concerns when he warned in 2018 that 'the prospect of machines with the discretion and power to take human life is morally repugnant'.[33] Opponents of these weapon systems allege that they will result in the 'dronification' of foreign affairs and the dehumanisation of warfare: because the use of drones reduces the need to deploy soldiers, political leaders might be more inclined to resort to force or escalation during a crisis, with war as the result. If both contestants possess such an arsenal, what happens when one of them runs out of these systems?[34] As a number of potential adversaries will certainly continue to field unmanned systems and develop military AI applications, NATO member states will need to recalibrate their capability portfolios to include defensive counter-drone capabilities and, given their increased vulnerability to drone attack, will need to reconsider which wars are worth fighting. The advent of military AI also raises military-strategic concerns, including how NATO should respond if Russia and China successfully integrate military AI and get inside Western OODA loops. NATO member states will therefore need to consider which military AI applications they want to develop and under which specific conditions they deem their use ethically acceptable.

[32] On the dynamics of European military innovation in the context of NATO transformation, see Terry Terriff, Frans Osinga and Theo Farrell (eds), *A Transformation Gap?: American Innovations and European Military Change* (Palo Alto, CA: Stanford University Press, 2010).

[33] António Guterres, 'Address to the General Assembly', 25 September 2018.

[34] Amitai Etzioni and Oren Etzioni, 'Pros and Cons of Autonomous Weapons Systems', *Military Review*, May 2017, pp. 71–81.

A related concern pertains to the deployment of immature AI to the battlefield, which would increase fog and friction and fuel unwanted escalatory spirals. The potential destabilising effects of the combination of new and, in some cases, untested technologies and their impact on the strategic balance of power, escalation dynamics and war presents another challenge. Emerging military space capabilities will pose a serious risk to the dynamics underlying deterrence in a multipolar world which are already under pressure due to a new generation of multiple independently targeted re-entry vehicles (MIRVs), the emergence of hypersonic (> Mach 5) missile gliders and the advent of global conventional prompt strike systems. If military powers can shut down the eyes and ears of adversaries by taking out their satellite systems, these adversaries may be unable to (fully) retaliate. This undermines credible deterrence and creates escalatory tendencies by giving parties an incentive to strike first. Ubiquitous surveillance systems (including space-based sensors) that are guided by AI and can reveal the location of nuclear missiles (even onboard submarines) increase this risk, as the accurate knowledge these systems provide might prompt pre-emptive strikes or deliberate escalation and risk-taking. Increasingly effective cyber attacks against nuclear C2 systems can likewise undermine deterrence. Hypersonic weapons (with conventional or nuclear pay loads), which can evade current state-of-the-art missile defence systems, may render C2 facilities, aircraft carriers and nuclear missile complexes vulnerable.[35] The potential unintended strategic consequences of each of the new technologies, and in particular the unpredictable effects of their deployment in combination, will certainly be topics of considerable political and societal debate within NATO's European populations that do not necessarily support increases in defence expenditures in general and increased spending on nuclear and unmanned capabilities in particular.

Conclusions and Recommendations

The evolving geopolitical context since 2014, with the intensification of strategic interstate competition, offers a strong incentive for NATO to explore the potential of these new technologies to maintain or as necessary even regain its military edge. At the same time, NATO must

[35] Keir A Lieber and Daryl G Press, 'The New Era of Counterforce: Technological Change and the Future of Nuclear Deterrence', *International Security* (Vol. 41, No. 4, Spring 2017), pp. 9–49; Michael C Horowitz, 'When Speed Kills: Lethal Autonomous Weapon Systems, Deterrence and Stability', *Journal of Strategic Studies* (Vol. 42, No. 6, 2019), pp. 764–88; Jesse T Wasson and Christopher E Bluesteen, 'Taking the Archers for Granted: Emerging Threats to Nuclear Weapon Delivery Systems', *Defence Studies* (Vol. 18, No. 4, October 2018), pp. 433–53.

modernise its non-controversial military capabilities to increase its conventional deterrence in the context of inevitable budgetary constraints. Moreover, while capability improvement is crucial in the context of strategic competition, the Alliance must also maintain sufficient capacity for peace operations, security force assistance and counterterrorist activities to address persistent threats and humanitarian security risks in the 'arc of instability' surrounding Europe. Against this background, this chapter yields, at a minimum, four recommendations.

First and foremost, NATO should review its overall capability portfolio and examine how it can strike a proper balance between restoring lost capabilities and pursuing incremental modernisation on the one hand, and more punctuated (some would say disruptive) innovation on the other.

Second, NATO member states must directly address the larger strategic, ethical, legal, technological and safety issues raised by emerging technologies. These issues should not be discussed in isolation and must be considered from a variety of perspectives. It is likely that these debates will expose distinct national policy positions regarding the legitimacy and desirability of new generations and types of weapon systems and the feasibility of developing and fielding them.

Third, NATO member states will need to prioritise modernisation and investments in advanced technology research, taking into account budgetary realities, national priorities and goals, the technological sophistication of their military forces and their industrial base and their geographic proximity to (perceived) threats. Not all states will be willing to participate in a strategic competition that plays out far outside NATO territory, as the debate on the NATO Strategic Concept of 2010 already revealed.[36]

Also, while NATO is of course sensibly monitoring the developments in AI, quantum computing and so forth, most of these emerging technology trends are driven by commercial actors such as Google and Microsoft. Because the development of AI relies on factors such as the availability of data, a skilled workforce, computing power and semiconductors, disparities in how well different countries can harness these technologies and can leverage the private sector may widen in the future.[37] Some division of labour is almost inevitable between those states that host high-tech companies and related research centres and those states that have fewer such resources but are in closer proximity to potential threats. The

[36] See Timo Noetzel and Benjamin Schreer, 'Does a Multi-Tier NATO Matter? The Atlantic Alliance and the Process of Strategic Change', *International Affairs* (Vol. 85, No. 2, 2009), pp. 211–26.

[37] Tomáš Valášek, 'New Perspectives on Shared Security: NATO's Next 70 Years', Carnegie Europe, November 2019, p. 36.

latter will likely see themselves forced to prioritise restoration of capabilities required for repairing NATO's deterrence posture in order to address their most pressing security problems.

Moreover, European states such as Poland, Finland and Sweden may be more interested in asymmetric solutions to emerging technological threats and may choose strategies emphasising defensive capabilities and boosting societal resilience. With regard to symmetrical responses to emerging military technologies, many European NATO members will probably see their dependence on US contributions and technologies increase rather than decrease. These considerations suggest that NATO needs to develop a realistic roadmap that allows for military modernisation among NATO member states at various speeds and with varying scope, while avoiding technical, tactical and doctrinal loss of interoperability and fostering a permissive political climate among the member states that recognises the military and political merits of such an approach.

Finally, the logic of modernisation and investment in emerging technologies will benefit from the development and adoption of a coherent operational concept that undergirds NATO's conventional deterrence posture. Military innovation theory strongly suggests that innovation succeeds when it focuses on actual and pressing strategic, operational or tactical problems.[38] Tactical problems abound in Europe. For instance, air–land integration capabilities require improvement for enabling traditional close air support in a contested environment in the Baltic region. Troops, in the context of both Article 5 and crisis management operations outside of Europe, need strengthened defences against threats posed by armed helicopters, fighter bombers, (swarms of) unmanned and autonomous weapon systems and surface-to-surface missiles. Russia's A2/AD capabilities deny NATO the air superiority that it requires for C4ISR purposes and that its thin line of ground troops in Eastern Europe rely upon. This can only be remedied through the development of new defensive and offensive capabilities and concepts of operations (which might, for instance, include cyber attacks or the employment of special operations forces assets). NATO also requires short-range, mobile air defences to counter intensive barrages of cruise missiles targeting NATO airbases, C2 centres, logistical hubs and other priority targets.

These issues, in turn, are part of the operational-level challenge of restoring conventional deterrence. Deterrence during the Cold War relied

[38] See Williamson Murray and Allan Millett (eds), *Military Innovation in the Interwar Period* (Cambridge: Cambridge University Press, 1995), Chapters 7 and 8.

not only on nuclear weapons, tanks, submarines and fighter aircraft but also on an operational concept that tied all of these together and was designed specifically to undermine the preferred strategy of NATO's adversary. During the 1970s and 1980s, the basis for military modernisation among NATO's militaries was provided by the concept of Follow-On Forces Attack and the rediscovery of manoeuvre warfare through AirLand Battle. These concepts clearly defined roles and missions in the various domains, which in turn provided the logic for weapon system development and procurement, and for investments in promising emerging technologies. While the US is exploring the merits and implications of Multi-Domain Operations, NATO currently lacks an equivalent overarching warfighting concept. This constitutes an important weakness.

All in all, emerging technologies that are integrated into the warfighting capabilities of various non-NATO military powers, along with the greatly strengthened power projection capabilities of non-state actors, add to the political and strategic challenges NATO faces. NATO must gear up to keep pace with the rapid rate of technological change and ready itself to protect NATO members against the security threats of tomorrow. After all, the truly prudent do not seek refuge when they see danger, they prepare.[39]

[39] BibleGateway, 'Proverbs 22:3', <https://www.biblegateway.com/passage/?search=Proverbs+22%3A3&version=NIV>, accessed 20 January 2020.