Report

The Future War, Strategy and Technology Conference

Monday 9 – Wednesday 11 October 2023 | WP3219

With sponorship from:

Wilton Park

Report

The Future War, Strategy and Technology Conference

TECHNOLOGY BEFORE FLESH: THE WESTERN WAY OF FUTURE WAR

Monday 9 – Wednesday 11 October 2023 | WP3219

In partnership with The Alphen Group, with major funding support from NATO and sponsorship from Anduril Industries, Syniad Innovations, Teledyne and Area9 Lyceum

Julian Lindley-French and David Richards
Wilton Park | October 2023

"If there is one critical change of command culture needed it is the development of cohesion-driven Alliance-wide, Partner-plus culture of automaticity of response".

Julian Lindley-French

List of Contents

Introduction

The Future War, Strategy and Technology Conference was specifically designed to complement the work of NATO Chief Scientist Dr Bryan Wells and his team, specifically, the NATO Science & Technology Trends 2023-2043 report by addressing a series of additional policy and strategy questions. What will be future requirements? What impact will emerging and disruptive technologies (EDTs) have on Allied and Partner forces, interoperability, and missions, and in what combination? What new and adaptive force concepts and doctrine will be needed? What political, military and defence-industrial policies and processes will be needed to enable our forces and at what scale? How should democracies conduct warfare with EDTs? What impact will EDTs have on the conflict escalation ladder? How must military innovation evolve to enable commanders and operators to test and experiment with EDTs and accelerate both capability and new concept development? For NATO, how will such developments impact the relationship between Allied Command Operations (ACO) and Allied Command Transformation (ACT)? How best to educate political and senior military leaders to help better prepare them for informed choices on defence policy, strategy and technology? How will EDTs better enable the human dimension of warfare? How have democracies integrated technology in their respective armed forces over the past 120 years? How will command and control and C4ISR change?

To address these questions, Wilton Park and The Alphen Group jointly organised this four-day, invitation only conference, bringing together some 80 leaders, experts, analysts and commentators from public policy and politics, the armed forces, the private sector, and from technology and innovation. Participants came from the democratic world across North America, Europe and Asia.

The conference methodology centred around eight working groups that considered the implications for defence and military strategy of EDTs: the Technology Working Group, Military Strategy and Future Force Working Group; Capabilities Working Group; Industrial Implications and Procurement Working Group; Strategy and Policy Working Group; Ethics and Legal Working Group; and Training and Leader Education Working Group. Finally, the Dreadnought Working Group considered the impact of the fusion of such technologies on future war. The conference considered two phases: now to 2035 and 2035 to 2050. Phase one is likely to see the enabling of the warfighter by such technologies, whilst beyond 2035 (phase two) autonomous action by such technologies is highly likely. These groups met for over six hours and constituted the key mechanism for delivering the conference outcomes.

Overarching Takeaway

There are two emergent, emerging, and disruptive technologies EDTs that will drive the changing character of future war: artificial intelligence (AI) and synthetic biology (synbio). Machine learning, big data, quantum computing and nanotechnologies will either drive or exploit these two framework technologies. Technology will thus shape strategy as much as strategy drives technology, not least because the defence establishment has so little control over technological development and application. There will also be two phases. Prior to 2035 such EDTs will play an essentially enabling role. Beyond 2035, as these technologies mature, they are likely to become increasingly autonomous. However, there is unlikely to be a ‘silver bullet’ technology that could lead to a ‘Digital Dreadnought’ breakthrough making all other platforms and systems simultaneously and immediately obsolete. Mass of force will thus continue to have as much an intrinsic quality in warfare as quality of force.

The next defence planning cycle will see ever greater application of such technologies as enablers of the warfighter, not his/her replacement. Beyond 2035, the sheer pace and scope of technological advancement could well see the rapid development of autonomous ‘intelligent’ systems, such as drone swarms and glide missile systems.

If the Alliance and its Partners are to maintain a critical comparative advantage over autocratic peer competitors, credible deterrence and defence will require NATO to understand far better the application and interactions of such technologies in the post-2035 future high-end battlespace. Only then can informed policy, strategy, and procurement decisions be made in conjunction with partners in the defence technological and industrial base. The failure to properly understand the utility of technology could be devastating. For example, the force President Putin thought he had available to him on the evening of February 23rd, 2022 was not in fact the force that existed because the Russian military had failed to integrate the technology they thought they had. This forced the Russians to shift from a concept of conquest to a concept of destruction in Ukraine.

Core Message

"We must think the Future".

"Substantial risks may arise from potential intentional misuse or unintended issues of control relating to alignment with human intent. These issues are in part because those capabilities are not fully understood and are therefore hard to predict. We are especially concerned by such risks in domains such as cybersecurity and biotechnology, as well as where frontier AI systems may amplify risks such as disinformation. There is potential for serious, even catastrophic, harm, either deliberate or unintentional, stemming from the most significant capabilities of these AI models. Given the rapid and uncertain rate of change of AI, and in the context of the acceleration of investment in technology, we affirm that deepening our understanding of these potential risks and of actions to address them is especially urgent".

The Bletchley Declaration, November 1, 2023

NATO's Worst-Case Mission

NATO's essential mission is to consider the worst-case and offer Allies and by extension Partners affordable solutions to meeting any such threat. Whilst much is made of the potentially transformative role of EDTs in the battlespace those charged with preparing for the future force have little real understanding of either their application or impact on strategy and doctrine. The result is that both strategy and doctrine are being driven by incomplete knowledge and imperfect data reinforced by misplaced confidence. This dangerous combination is due in no small part because technological innovation is no longer driven by defence establishments in democracies but rather by the commercial sector.

The Conference validated the work of the Chief Scientist and his team, specifically *Technology Trends 2023-2043*. Artificial Intelligence, autonomous systems, big data, information and communication technologies, energy and propulsion systems, hypersonic systems, space-based capabilities, quantum technologies, human-performance enhancement, novel materials and advanced manufacturing and other 'exotic' technologies will doubtless impact the Western Way of War but how, to what extent and when is not known and very little understood. Changing that is now critical and a capstone requirement.

Demonstrably maintaining and gaining comparative advantage is the *sine qua non* of Allied deterrence and defence. If Allies and Partners are to gain comparative advantage today and tomorrow in both deterrence and defence, it will be vital to establish a new defence eco-system in which public and private sectors work closely and innovatively together at speed. The focus should thus be on the end-user of technology reinforced by an agile system of responding to feedback, need, and the evolving capabilities of the adversary.

The years 2023 and 2024 are a critical moment in Alliance planning. NATO must seize the moment given that that 2023 is “Year 2/Step 2”in the current (2022-2026) NATO Defense Planning Process (NDPP) cycle (2022-2026) during which capabilities must be identified to ensure that the Capabilities Target (CT) “package” is presented to Heads of State and Government for final endorsement at the July Washington 2024 Summit. As such, it is vital that the Alliance capture not only the lessons learned from the Russo-Ukraine War, especially about UAVs and UCAVs, establishing the appropriate requirements definition for sustained production lines, and for the development of emerging and disruptive technologies that are beginning to appear from technology innovation initiatives such as DIANA. It is also vital that the capabilities targets are distributed to all Allies in 2024 prior to the summit under the rubric of the NDPP "Year 3/Step 3”, i.e. allocation of requirements, consistent with NATO’s principle of fair burden sharing and reasonable challenge. This will be vital to deflect critics in the US at a particularly sensitive moment in the political cycle who assert that Europeans are not taking on an appropriate share of the overall Alliance burden.

Consequently, there can be no room for complacency. Ernest Rutherford once warned that splitting the atom might lead to a catastrophe. Some at the cutting edge of AI are similarly concerned. In 2023, Elon Musk joined others to call for a hiatus in development until the risks are better understood. Prof Yoshua Bengio, seen as a leader in the AI community, also warned that he would have placed safety over utility had he understood how fast the technology is developing. That very statement captures the paradox of EDTs – those developing it have a vastly better understanding of its applications – good and ill – than those in government who will be responsible for ordering it and applying it.

A Fleet of Digital Dreadnoughts?

The simple truth is that no-one really understands how EDTs will develop and few policymakers have the imagination to envision future war particularly when AI is fused with other technologies to possibly realise a Digital Dreadnought moment, or rather a fleet of Digital Dreadnoughts moment when the fusion of such technologies affords an actor a decisive military breakthrough that for a critical period would give the attacker a war-winning advantage over the defender.

Therefore, NATO, its Allies and Partners urgently need to commission further studies by the Chief Scientist to do precisely that – better understand such technologies, their applications and their possible fusions. Eighty years ago, the development of atomic science led to both abundant energy and the first weapon of mass destruction. However, a lack of understanding in cash-strapped European governments has bred cynicism in power about breakthrough scientific and industrial innovation. This so-called ‘precautionary principle’ tends to emphasise caution before any potentially revolutionary technology is exploited. The West’s adversaries?

What is clear is that the changing character of warfare is facing not just a set of force multipliers but immeasurable magnifiers. The hard truth is that many Western governments have also enshrined the precautionary principle into a ‘not-spending money’ principle on the grounds that few ‘fancy gadgets’ ever work. This culture of governance has too often stifled innovation and led to controversial decisions, such as the ban in some countries on genetic modification (GM) for reasons that are little more compelling than the burning of medieval witches. Secretary-General Lord Robertson once rightly said it is all about “capabilities, capabilities, capabilities”, but such capabilities cannot be generated until there is an understanding of technology and its relationship between defence and military strategy! Moreover, sooner or later ‘new’ tech becomes old tech and inevitably spreads. AI, machine learning, quantum computing etc cannot be un-invented, and if the Western democracies do not exploit them others will.

Why Now?

Why now? NATO Allies and its Partners the world-over are engaged in systemic competition with autocratic states such as China and Russia. Russia seems determined to contest the sovereignty of Allies and Partners by seeking to dominate, coerce or even conquer territory. China is developing a very muscular military instrument of power (MIoP) and it is reasonable to assume that within 7-10 years Russia will have reconstituted the damaged elements of its armed forces and developed those not as yet engaged in Ukraine. It is also reasonable to assume that both China and Russia will further exploit emerging and disruptive technologies across the hybrid, cyber and in time hyperwar spectrum.

Much of that competition will be played out in the race to develop and apply EDTs to strong effect in the future force and future battlespace. An arms race is already underway, and the democracies need to engage and win. Emerging and disruptive technologies will help to re-define the character of high-end war, if not its nature, and thus establish the basic requirements for maintaining credible deterrence and defence going forward. Speed of recognition, autonomy of decision and distributed command will be its quintessence across the multi-domains of a four-dimensional battlespace in which the analogue and the digital will co-exist. In time such technology could lead to hyperwar: warfare led by AI in which humans have little command agency. Too many policymakers and practitioners understand little about the potential impact on the battlespace of AI, quantum computing, machine-learning, big data, Synbio, nanotechnologies, 'intelligent' autonomous drone and unmanned vehicles, as well as hypersonic and glide missile systems and a host of other technologies.

Both the NATO Communication and Information Agency (NCIA) and the Office of the Chief Information Officer (OCIO) show that it is possible to speed up processes for acquisition of technology and software. Hitherto, NATO processes and those of most Allied defence ministries would take four years but that is being reduced to one year, although the private sector still takes only four months. What is important is that a mix of imagination and agility has enabled NATO for the first time to lead across defence on the speeding up of technology acquisition. In other words, it is possible a precedent for action has been established proving the Alliance can improve the speed of acquisition but only through close industry partnering and access to commercial sector know how.

Strategic and tactical imagination will be vital and there is already innovative developments and new thinking within the broader compass of the Alliance. For example, a 2031 NATO-relevant scenario at the 2023 Gartner Defence Symposium envisaged the Joint Expeditionary Force (JEF) engaged on a multi-domain operation in which an AI-administered biosynthetic antidote is used to prevent a nerve attack on the commander, and during which an autonomous container ship with a reinforced biosynthetic light hull designed for operating in Arctic ice sludge is boarded and then sunk by Russian forces. At the same time, mass cyber-attacks take place on hospital ventilators and physical attacks on critical underwater infrastructure. However, all the attacks are countered and defeated by a rapid thinking multinational headquarters equipped and staffed in partnership with industry cooperation because of new sourcing strategies that NATO is already piloting guaranteed by financing from the JEF bank concept.

People Protection and Power Projection

Protection of people will also be as important as projection of power. The development of EDTs will again place the security of the home base at a premium because future war will likely be a form of total war in which all citizens will be engaged. If society is vulnerable the capacity of democratic states to project power will be profoundly constrained, and future deterrence and defence will depend on a capacity to project as well as resist coercive power. The first step is to make society more information resilient by educating people to identify fake news.

Critically, all democratic societies will soon need to make hard choices as to which technologies are most relevant and how they might be harnessed collectively as they design and implement their respective future deterrence and defence postures. In NATO they have no better tool to collectively undertake such an endeavour. If they do not, China, Russia and others will press ahead forcing the democracies to react rather than lead. In time, they could all face a “Dreadnought” moment in which EDT is tailored in such a way as to create an era-defining weapons systems that renders Allied and Partner deterrence and defence obsolete at a stroke and digitally decapitates government and governance in such a shocking way that defeat is suffered before any war is fought.

Executive Summary

Future War, Strategy and Technology

1. The challenge posed to the Alliance by EDTs exists across the three re-conceived NATO core tasks of deterrence and defence, crisis management, and co-operative security. The sine qua non of future Allied deterrence and defence will be a military instrument of power that is ready for the threat posed by Russia, the consequences of a rising, militarist China, as well as destabilising risks below the threshold of war around the 360-degree periphery of the Euro-Atlantic area. Europeans and Partners in the Indo-Pacific will also need to develop far stronger military capabilities to ease growing pressures on US armed forces. Technology will be one solution in striking a new balance between mass and manoeuvre, quantity, and quality, but technology will not offset a lack of quantity. There is no silver bullet.
2. Day one interoperability is still a very significant challenge for Allied and Partner forces. As devolved command authority becomes ever more prevalent campaign and mission success will rely on secure and seamless data-sharing at the high end of interoperability when command and force structures are under intense pressure and over time increasingly reliant on AI-driven data integrity. Allied and Partner forces need far greater “adaptation readiness” supported by policies that enable Western governments to better exploit technology. This assessment is supported by lessons from the Russo-Ukraine War which suggest that during the next defence planning cycle (10-15 years) emerging and disruptive technologies will be applied alongside existing platforms and systems such as artillery and armour to better enable them.
3. Multi-domain operations (MDO) involve integrated actions across air, sea, land, cyber and space with the critical relationship being that between sensors and command and control systems. It will be vital that SHAPE develops as a strategic warfighting headquarters designed to exert effective and upscaled command and control over such a complex and technologically driven concept of operations. The objective must always be to ensure SHAPE remains militarily fit across all and any threats it may face, which means a retained and proven capacity to analyse, advise, develop appropriate strategic approaches, plan, resource, command and control the fight, assess, and validate.
4. These missions will become ever more challenging given the marked acceleration in the Observe, Orient, Decide, Act (OODA) loop that is taking place. For example, plans must not only be updated constantly they must also be resourced, which places a particular premium on prioritisation, particularly where it concerns the use and utility of technology. For the future warrior to be effective therein, information and knowledge will be as important as capabilities and thus an integral part of multi-domain operations with a proven capacity to act at the speed of relevance. The credibility of NATO’s future deterrence will be reliant on such responsiveness.

5. The lessons-learned process will be particularly important as much of it will become technology-enabled. Such lessons will also need to be drawn from across a much broader spectrum given the scope and nature of multi-domain operations with doctrine development and professional military education particularly important to maintain force and operational cohesion together with effective decision-making and agile command and control.

6. If industry is to meet the demand of technological change AND the upscaling of production needed an EDT industrial strategy is required that will in turn be dependent on secure sources of vital raw materials and new productive capacity. Any such industrial strategy must be necessarily focused on the defence primes within the respective defence, technology, and industrial bases of Allies and Partners, but must also be extended into new sectors of industry and involve companies that have hitherto had little engagement with the defence sector. New supply chains will also be created that will need to be protected, a significant part of which will involve a 're-shoring' of the defence-relevant industrial base.

7. Where will the money come from? Adaptation of Allied and Partner forces will require very significant investment and will not be possible without the immersion into policy of industry and private sector investment across EDTs, particularly where it is the civilian sector driving much of the technological innovation. Government investment will be vital to 'seed' technological development because commercial markets are unlikely to invest in projects that have a maturation beyond 5 years.

8. Given the likely scale of requirement and the depth of partnerships needed if Allied and Partner governments are to secure private investment at scale, governments must themselves been seen to give defence a far higher political priority than hitherto and make commitments to the medium and longer term. At the very least, governments will need to adopt a whole of government investment approach and create tax incentives for the development of nationally critical technologies. A new legal framework will also be needed together with incentives for the commercial sector to become a partner in updating systems and software regularly. For example, to promote such agility US Special Operations Command (SOCOM) has adopted the practice of Transition Confidence Levers.

Future War and NATO

9. As EDT is adopted forces must develop a mission command focus and be exercised to the point of failure. This is because devolved command authority will become increasingly the norm. Survivability of command will be an essential pre-requisite for mission success. At present, large Allied headquarters generate a very significant heat and electronic signature and are thus extremely vulnerable to attack. Moreover, if devolved command authority is to be credible there are two other domains that will be vital to mission success – information and knowledge. Time critical and information hungry systems will require intelligence and information sharing closer to Five Eyes levels of trust than current Alliance procedures.

10. "The NATO Defence Planning Process (NDPP) is not fit for purpose in dealing with technological change which is far faster". The Alliance must create a system that enables Allies to inject technology far faster into the NDPP. Planning and procurement will need to become far more closely aligned and more secure across the Alliance. Moreover, the NDPP and Allies must also be adapted to cope with asymmetric technology cycles. For example, the development of new software can take a matter of months, whereas some systems take 2-3 years whilst platforms in many Allied and Partner countries can take up to 20 years to field.

11. “Too many Allied and Partner defence bureaucracies remain resistant to change”. If more agile mind-sets are to becomes the norm ‘Red-Teaming’ of decisions and plans will be vital and could well be a critical advantage. China is facing a raft of problems due to the inability of Beijing to cope with its own internal diversity. Chinese organisational culture is incapable of employing reinforcing and positive criticism. This is an area where Allies and Partners could generate a critical comparative advantage, but it will also require an overhaul of professional military education with technology applied to knowledge generation at all levels of command.

12. By the mid-2030s it is reasonable to assume that emerging and disruptive technologies in the battlespace will lead to intelligent, digitised, interconnected, and yet distributed applications of force and resource on a scale, speed and scope hitherto unknown. Artificial Intelligence, machine learning, synthetic biology, nanotechnology and in time quantum computing are already changing society. They will also change the battlespace because such technologies will drive military strategy as much as strategy drives technology.

13. Equally, it is unlikely technology will offer a silver bullet that can offset a failure of NATO Allies and Partners to invest in sufficiently capable armed forces at a size appropriate to the threats they must confront. The Russo-Ukraine War is again proving that mass is a quality. What is needed are informed and intelligent choices to be made about the application of such technology in maintaining credible and legitimate deterrence, defence, and security.

14. If intelligent choices are to be made about which technologies in which to invest it is vital such choices are made in partnership with stakeholders responsible for the conduct of strategy. The fusion of strategy with technology will take place as part of capabilities development, military strategy, future force planning, the adaptation of the defence, technological and industrial base, key leader education, professional military education and within ethical and legal frameworks. Any such choices must thus be dependent on a new and much more assured relationship between Allies and Partners and between government and industry. This is because the Alliance and its Partners are entering a phase of multi-domain high-end deterrence and defence that will reach across air, sea, land, cyber and space and built on the ability to detect, determine and drive proportionate actions very fast.

The Military Applications of Emerging and Disruptive Technology

15. The 2022 Future War and Deterrence Conference Report stated that, “By 2035, at the very latest, it is reasonable to assume that everywhere will be a battlefield and everything will be a weapon. Therefore, and at the very least, Europeans will need a high-end, first responder force that can act from seabed to space and across the domains of air, sea, land, cyber, space plus information and knowledge. A force of sufficient twenty-first century manoeuvre to be able to respond to any threat from the Arctic to the Mediterranean should the US be engaged in strength elsewhere. A force also of sufficient mass to simultaneously support front-line Allies and Partners in dealing with significant insurgencies and emergencies”.

16. A force incorporating and leveraging EDTs that are AI, autonomous systems (including drone swarms), big data, information and communication technologies, energy and propulsion technologies, hypersonic systems, electronic and electromagnetic technologies, space-based capabilities (including commercial capabilities) from imagery to tracking and beyond, and the future role of quantum technologies, novel materials and advanced manufacturing, and military personnel that are physically and perhaps cognitively enhanced. Western forces will have to

counter adversarial use of these enabling technologies, and such adversaries may not adhere to their ethical, legal, and moral norms. The true test will be interoperability among Allies and with the US future force and those of Partners in Europe and the Indo-Pacific at the high-end of conflict and under extreme duress.

Artificial Intelligence

17. AI will over time enable autonomous and high-speed weapons. AI-enabled systems will defend networks, computers, programmes, and data and respond by rapidly developing a tailored response to all forms of cyber-attack and counterattack. The challenge will be to attribute attacks. AI is central to the development of the Internet-of-Things which links everyday devices through sensors and data-processing to communicate with each other. Such devices are becoming an ever more influential part of everyday life. If such systems were to suffer a systemic attack, they could see the effective collapse of society if such an attack also took place in conjunction with the destruction of critical national infrastructures. AI will also be critical for the secure transportation of goods, ammunition, armaments, and troops and will thus be an essential enabler for future military operations through enhanced efficiencies. AI will also enable military systems to detect anomalies and predict failures.

18. Intelligence, Surveillance, and Reconnaissance (ISR) is increasingly reliant on AI to acquire and process information vital to military operations. For example, there are a host of unmanned systems that can undertake ISR missions autonomously enabling both strategic and tactical threat monitoring. Soon, AI ‘intelligent’ unmanned aerial vehicles (UAVs/drones) will not only autonomously identify potential threats but warn forces as well as engage the threat. The pace of development of such systems depends on the combined application of AI, machine-learning, and quantum computing. It is that combination which could realise a new Digital Dreadnought moment.

19. AI, machine learning and super-computing already enhance target recognition by rapidly improving command understanding of operational challenges through corralling and collating reports, documents, and unstructured information into easily understandable messaging. AI also helps identify targets and forecasts enemy actions and responses. AI can also offer a more granulated picture of weather conditions, ensure supply systems remain optimised, and offer a range of command options.

20. Over 30% of medicines over the next 5 years will be designed by commercial AI software which means bio-threats will also accelerate and thus make bio-warfare both more accessible and affordable. On the plus side Robotic Surgical Systems (RSS) and Robotic Ground Platforms (RGPs) will increasingly enable remote surgery as well as a host of other vital medical support. Perhaps the greatest near-term impact of AI on the way armed forces do business is in defence education and training by promoting a host of remote training and distant education possibilities with real time support for deployed forces.

Synthetic Biology and Human Enhancement

21. Synthetic biology combines living systems and organisms and applied engineering principles to enhance human performance. Much of the work concerns nanotechnologies, which combine material science, chemistry, biology, and engineering down to the molecular level. Synbio also seeks to augment the natural capabilities and capacities of the warfighter by manipulating biology to increase and enhance protection, situational awareness and lethality.

22. Future war applications will range from the use of extremely small robots, hyper-reactive explosives, and electromagnetic super-materials. Further developments are also taking place in aerospace and reinforcing armoured protection as well as lightweight, flexible, and highly durable materials reinforced by sensors.

Cyber

23. In August 2019 NATO Secretary-General Jens Stoltenberg stated that "A serious cyberattack could trigger Article 5, where an attack against one ally is treated as an attack against all". Cyber warfare is usually defined as a cyber-attack or series of attacks that target a country. It has the potential to wreak havoc on government and civilian and military infrastructures and disrupt critical systems to such an extent it could result in damage to the state and even loss of life. Cyber warfare typically involves a nation-state perpetrating cyber-attacks on another, but in some cases the attacks are carried out by terrorist organisations or non-state actors seeking to further the goal of a hostile nation. There is no universal, formal definition for how a cyber-attack may constitute an act of war.

24. Cyberspace has also been designated a domain in which the Alliance will operate and defend itself as it does in the air, on land, and at sea. NATO will thus deter and defend against aggression both in the physical and the virtual. To that end, NATO has established a new Cyberspace Operations Centre in Mons to increase cyber situational awareness. This capability is reinforced by national cyber capabilities.

25. Cyber espionage involves the use of botnets or spear phishing attacks to compromise sensitive computer systems and steal proprietary information. Both China and Russia are engaged in extensive operations against Allied and Partner states. Espionage and sabotage are closely linked with adversaries and terrorist groups seeking not only to steal information but also to destroy it.

26. Offensive cyber actions include potentially mass disruptive denial-of-service (DoS) attacks which 'crash' systems by forcing websites to become overloaded with fake requests, thus disrupting critical cyber operations and systems and preventing critical civilian and military authorities from acting at the top of government. As cyber war escalates hostile forces could attack power grids, communications networks, health systems and other critical infrastructures upon which democratic open societies rely.

27. One of the most pervasive forms of attack on open societies is cyber-enabled information warfare. Civilians and military personnel are under constant pressure in social media from efforts to influence their belief systems and undermine the cohesion of democratic states. Most modern economies are overwhelmingly digital and hostile forces routinely target ministries and corporations, most notably stock markets, payment systems, and banks. The worst case would be a systemic surprise cyber-attack, in effect a digital Pearl Harbor or 9/11 that would be a massive 'out of the blue' attack, possibly in conjunction with a physical attack or wider hybrid warfare.

Quantum Computing

28. Quantum computing combines quantum physics, computer science and the theory of information to decrease the number of operations needed to calculate at ever greater speeds and at far lower levels of energy use. Future quantum computing will be at the core of machine learning, big data analytics and AI and is the most likely core component of the kind of technology fusion that leads to a "Digital Dreadnought" moment. However, quantum computing (QC) is perhaps the most over-sold and yet to be realised technology. As of November 2023, no quantum computer can out-perform a 'conventional' super-computer and the technology faces a host of engineering and systems challenges before the undoubted potential such a machine would afford the first to develop and apply it in the real world. In theory, the advantage of quantum computing is the sheer amount of data it could process, the

speed it could process that data, and the possibility such a system could in time make autonomous decisions.

29. In time, quantum computing will enable machine-learning, but it is also a voracious consumer of both of historical data and real time information, precisely so it can 'learn' how the data patterns evolve to identify trends over time. The challenge is that as the volume of data increases, so will the very complexity of the data and the sheer scale of it, thus making it necessary for the system itself to generate said data independent of any operator.

30. There are quantum computers in existence, such as Google Sycamore, which has reportedly solved a problem in 200 seconds that would have taken today's fastest supercomputer 10,000 years to solve. If true, such a capacity could have a range of military applications. At the very least, early military applications are likely to be focused on quantum sensing and secure communications, cryptographic decoding, cryptanalysis, AI/pattern recognition and bioinformatics to analyse bioweapons so that countermeasures could be stepped up rapidly.

Adversarial Machine-Learning

31. Machine learning is the use and development of computer systems that can learn and adapt without explicit instructions by using algorithms and data patterns to draw inferences. To be effective in the battlespace machine learning will need to become intrinsically more robust before good use can be made of it in, for example, scenarios with increasingly intelligent and adaptive opponents.

32. In time, machine learning tools will be applied across the whole spectrum of military operations, from improved strategic thinking down to low-level tactical applications, like controlling swarms of autonomous unmanned weapons systems. However, some of the most influential applications in a military theatre could be felt away from the battlefield. Chinese military strategy includes the aim of using machine learning to achieve superiority across the electromagnetic spectrum. Developing faster, more insightful machine-learning led AI could clearly enable one side to enhance the communications and situational awareness of their forces, whilst enabling them to disrupt, degrade and deny those of their adversary.

33. Machine learning and deep learning are two sides of the same coin. The rapid progress in deep learning techniques affords an ability to analyse different kinds of images and data from heterogeneous sensors, which is why this technology is particularly interesting for military and defence applications. As yet, many machine learning systems are unable to compete with intelligent opponents, which could make such systems vulnerable to the ones that are.

34. Adversarial machine learning will be particularly important if opposing forces can make machine learning systems useless or even dangerous for those relying on them. Other military applications of adversarial machine learning systems include camouflaging adversarial algorithms to hide military aircraft or land vehicles from drones and satellites equipped with systems based on artificial intelligence. Similarly, missiles guided by deep learning algorithms could be deceived by adversarial data and diverted to other targets. DARPA has recently launched several important projects focused on the use of adversarial machine learning such as the GARD (Guaranteeing AI Robustness against Deception) programme. GARD operates on a four-year plan and is designed to study the theoretical foundations useful for the design of more robust machine learning algorithms, the creation of defence algorithms from adversarial data and the creation of test frameworks.

The Changing Nuclear Threat and Next Generation Weapons

Nuclear Weapons

35. Today, there are nine nuclear weapons states; the US, Russia, UK, France and China plus India, Pakistan, North Korea, and Israel. Iran and Saudi Arabia are also seeking such a capability. Russia is no longer participating in the START 2 treaty, which is due to expire in 2026 and unlikely to be renewed. China refuses all and any such constraints and aims to increase its nuclear arsenal from some 400 warheads today to over 1500 by 2035. The UK is also building a new generation of four Dreadnought class nuclear ballistic missile submarines and the US is considering once again placing nuclear weapons in Britain at RAF Lakenheath, as part of a "potential surety mission".

36. Whilst Beijing and Moscow routinely exaggerate the technological advances they are making in manoeuvrable re-entry vehicles and air-breathing manoeuvre technologies (MARV), China and Russia are developing systems designed to overcome any potential strategic missile defence. Much of the effort to create advanced MARV systems involves hypersonic capabilities, which combine elements of both ballistic and low trajectory strikes at speeds over Mach 10. For example. The Russian *Avangard* system is launched as a ballistic missile but then goes into an extended hypersonic glide, which means it can only be detected at the very end of its mission. Moreover, the combination of ICBM technology and hypersonic glide is also being reinforced by the development of MARV technology. *Fractional Orbital Flight* technology increases the challenge for any defence exponentially.

Directed Energy Weapons

37. Directed-energy weapons (DEW) uses concentrated and focused energy to incapacitate or destroy targets. Lasers, microwaves, and particle energy beams are the most common such systems and are designed to strike personnel, incoming missiles, vehicles and optical ranging equipment. The US is also developing electro-magnetic railguns as part of a new multi-layered defence again ballistic, hypersonic, and hypersonic glide missiles and vehicles and could be deployed as early as 2025.

38. Russia, China, India, and the UK are also developing such systems. Iran claims to have an operating system whilst Turkey says it used an ALKA directed energy system in Libya in August 2019. The advantages of directed energy weapons are manifold. Radiation beyond the visible spectrum is undetectable and they are silent and unaffected by climatic factors such as wind. The main limiting factor is dispersal of the beam over distance. Lasers operate at the speed of light and in time could be effective in space as an anti-satellite weapon. They do not necessarily need large logistics support but do need a lot of energy and the means to generate it, which makes ships the most convenient 'host' for such systems.

39. There are also *microwave weapons* under development for both anti-personnel and equipment use (even down to the low tactical level) with the US developing the Counter-Electronics Microwave High-Powered Advanced Missile Project as part of future missile defence. *Particle-beam weapons* use charged or neutral particles to attack targets both in the Earth's atmosphere and beyond but are vulnerable to what is called 'blooming' – the dispersal of the particle beam. *Plasma weapons* discharge a stream of particles made up of dynamic matter comprised of electrons and other particles. The MARAUDER project is one such example designed to discharge an extremely brief but concentrated and large amount of directed energy. *Sonic weapons*, as the name suggests, use disruptive low frequency tones to damage human brains.

Proceedings

"There is a new digital fog of war".

Conference Mission and Scope

40. Carl von Clausewitz identified five components of military strategy: the moral, physical, statistics, mathematical and geographical. There is also the technological. The Future War, Strategy and Technology Conference examined seven distinct but linked tracks of analysis: strategy and future force; technology, innovation, capability requirement and capability-development; policy; ethical and legal; training and education.

41. For the Alliance, there are several questions that it must address. What EDTs will be relevant and have offensive and defensive military utility? What impact will such technologies have on military strategy, doctrine, concepts, tactics, training, education, and personnel? How should such technologies be developed and procured and what parameters should inform such choices? What future balance will Allies and Partners need to strike between resilience, security of information, and defensive/offensive capability? What relationships must be forged between the private sector (industry and academia), government, and the military for optimum improvements in security and defence?

42. There are five working imperatives for shaping future war: cognitive superiority, resilience, power projection, command and control, and cross-domain defence. Technology will be vital in assuredly accelerating decision-making, protecting information and dominating a new escalation ladder that will incorporate conventional force, cyber force, and nuclear force.

The Future War, Strategy and Technology Challenge

43. The focus of the conference was on the relationship between the NATO MIoP, the threats and missions of the Alliance, and emerging and disruptive technologies. For the Alliance this manifold challenge is implicit in the three re-conceived NATO core tasks of deterrence and defence, crisis management, and co-operative security, which are today very different in both scale and complexity than when first conceived in 2010. The *sine qua non* of future Allied deterrence and defence will thus be a MIoP that is ready for the threat posed by Russia, able to contend with the geopolitical, military, and technological consequences of a rising, militarist China, whilst also able to confront and master a gamut of destabilising below the threshold of war risks around the 360-degree periphery of the Euro-Atlantic area. Given the complexity of such a challenge the MIoP will only be effective if it is embedded in a Comprehensive Instrument of Power (CIOP) concept by which all forms of statecraft are applied.

44. A core assumption was that Europeans and Partners in the Indo-Pacific will at the very least need to develop far stronger, more agile, capable, and sustainable military forces to ease growing pressures on US armed forces and maintain interoperability with the Americans at all levels of conflict but most importantly at the high-end when forces are under intense command duress. Technology will not only be a vital enabler of such future forces but will be equally vital in further enabling the Allies and Partners to strike a new balance between mass and manoeuvre, quantity, and quality.

45. The Russo-Ukraine War has also demonstrated that mass of force still matters and has a quality of its own. Therefore, the Alliance must meet the threat of mass as well as technology-enabled manoeuvre precisely because EDTs will afford adversaries the capacity to challenge NATO Allies and Partners across borders, regions, and the multiple domains of the future battlespace across air, sea, land, space, cyber, speed of information and assured application of knowledge.

46. Effective multi-domain operations (MDO) will depend on robust cross-domain command structures, which must in turn be closely co-ordinated and where possible integrated with civilian domains because protecting people will be as important as projecting power. Indeed, they are two sides of the same collective security/collective defence coin. Consequently, the breadth of technology will be as important as the pace of its development. It will be hard for democracies to project stabilising power if the home base lacks resilience and protection. These missions will become ever more challenging given the marked acceleration of the OODA loop that is taking place. For example, plans must not only be updated constantly; they must also be resourced, which places a particular premium on prioritisation, even more so where it concerns the use and utility of technology. For the future warrior to be effective therein, information and knowledge will be as important as capabilities and thus an integral part of multi-domain operations with a proven capacity to act at the speed of relevance. The credibility of NATO's future deterrence will be reliant on such responsiveness.

47. The lessons-learned process will be particularly important as much of it will become technology-enabled. Such lessons will also need to be drawn from across a much broader spectrum given the scope and nature of multi-domain operations, with doctrine development and professional military education particularly important to maintain force and operational cohesion as well as effective decision-making and agile command and control.

48. Unfortunately, such adaptation will also place a premium on skill sets for which the Allied Future Force will continue to face recruitment problems given the allure of the civilian technology sector and other tech-dependant industries. New terms (and contracts) of service will need to be considered given that technology will be the capability-multiplier in an era in which the military instrument of power will rapidly become data-centric rather than platform-centric.

49. Applied innovation must be sought if the Allies and Partners are to achieve the three imperatives of future war: information dominance, command dominance and engagement dominance. Innovation will profoundly change force structures, not least vulnerable personnel-heavy deployed headquarters. Other shibboleths will also need to be abandoned, such as the idea that there can be no defence of Europe without the Americans. Rather, the future war, future defence of Europe will require a layered defence across a broad civil-military spectrum of activities and much of that effort will need to be European.

50. Innovation needs to be championed because it is always challenged within the Alliance on the basis that "the urgent always overcomes the important". Therefore, transformation should not simply concern the exotic and new but also employing EDTs intelligently to enable existing platforms. Human-machine interaction should be a priority because it is increasingly important. Such a phased and measured approach will be the only way to eventually realise the application of more exotic technologies in support of Allies and Partners.

51. Realising even modest outcomes will require all the NATO nations and those Partners willing to join the Alliance on this journey to work together to cross the hard yards of harmonisation, standardisation and interoperability which will be the quintessence of the twenty-first century Alliance. Such outcomes will be further dependent on a close and transformed relationship between the military instrument of power and the respective defence and technological bases of both Allies and Partners. Far more seamless interaction between them is needed than hitherto, as it is vital the technology sector become synergistic competitors – both competitors and partners in the development of defence capabilities. Only then will fielding times of both platforms and data-centric systems be aligned with the planning goals in, for example, the NATO Defence Planning Process (NDPP).

From Here to e-Technology

"There will be technology wake-up moments."

52. There are immediate lessons from the Russo-Ukraine War that also point to the future and warfare development imperatives based on cognitive superiority, layered resilience and influence and power projection. The utility of force will be increasingly reliant on increasingly distributed, interconnected, and intelligent digital systems. Despite the pressing need for change if not transformation in defence implied by the Russo-Ukraine War, there is still more continuity than change across leadership, logistics, industrial and political spheres.

53. The 2022 NATO Strategic Concept and the 2019 Military Strategy are, in effect, plans for two phases of development much of which will need to run concurrently. Phase one involves identifying and learning the lessons of the Ukraine War to bolster deterrence, defence, and resilience in the short-term. Phase two entails understanding, developing, and then applying controlled but autonomous-capable systems.

54. However, for all the advantages that EDT suggests, war will always remain a giant black hole into which people and materiel vanish at an alarming rate far beyond that envisaged by peacetime establishments. Whatever the adopted technology, NATO European forces will thus need far more robust logistics forward deployed, with enhanced and far more secure military supply chains particularly important. Far more materiel will also be needed, most notably ammunition.

55. Furthermore, if NATO deterrence and defence are to be credible within the framework of the Strategy Concept, Allies will need to rebuild and build infrastructure to assist military mobility and remove all legal impediments to rapid cross border movements in a pre-war emergency, including the movement of dangerous materials. Deployed NATO forces will also require much improved force protection with the need to reduce the detectability and thus digital footprint of force concentrations ('bright butterflies') paramount.

56. The war in Ukraine has revealed the vulnerability of armour unsupported by infantry and helicopters in the battlespace, as well as the need for NATO forces to be able to dominate both fires and counter-fires. Much of the vulnerability of Russian forces is due to the effectiveness of expendable drones, strike drones and loitering systems allied to precision-guided munitions. NATO forces need an awful lot more of all such systems across the tactical and the strategic. Enhanced land-based, protected battlefield mobility will also be needed together with increased force command resilience given how often the Ukrainians have been able to detect and 'kill' Russian forward (and less forward) deployed headquarters.

57. Thankfully, given that NATO is a defensive alliance, the war in Ukraine has also revealed the extent to which the defence has dominated the offence if forces are reasonably matched. Whilst no-one envisages a return to the twenty-first century equivalent of the Maginot Line, secure pre-positioned capabilities and access to individual ready reserves will be vital. There is one other lesson NATO leaders and commanders need to learn given the attritional nature of the war: do not sacrifice significant mass to afford a little manoeuvre.

58. A "transformative trinity" will also be needed if technology is to be harnessed to effect based on a common operating picture, which will in turn be critical for effective and yet complex multi-domain operations. The trinity will incorporate the "nesting" of civil and military assessments to provide a holistic view of the battlefield; the development of a system of systems approach and more devolved command and control (C2); and the ubiquity of autonomous systems across the maritime, land and air domains. Exploiting such EDTs will lead in time to strategic command that is at the edge of technology, and command and control will need to be able to cope with the

complexity that it will generate if it is to retain speed of relevance. A twenty-first century version of flexible response will thus demand twenty-first century flat and agile command structures. However, any such adaptation will also require the "intellectual reinvigoration" of the pursuit of arms with a wholly new way of thinking about how to mobilise force and resource in democratic societies.

59. Unfortunately, despite some signs of innovation Western armed forces are not very good at adopting new technologies. For example, the development of synthetic biology technologies "is a revolution" already underway and has great potential for enhancing human genius. However, it is very little understood by military establishments because they lack "technological literacy". If they do not understand the scope of new technologies, they cannot make informed and affordable decisions. Western powers also too often lack the ability to integrate existing technologies into military use whilst developing 'new' technology that is unable to deal with existing threats, such as hypersonic missiles.

60. Therefore, before any judgements can be made over future technological requirements and with them any realistic aspirations for a properly integrated future force, forecasting needs to be markedly improved across the conflict spectrum. That goal will also mean a new balance must be struck between the high-end forces needed to deter Russia and the counterinsurgency forces that could be needed to engage state collapse in the Middle East and North Africa. Both scenarios have profound implications for the security and stability of Europe.

61. Equally, steps need to be taken now, and that means putting the right people in the right jobs with the right brief now. The excellent NATO Warfighting Capstone Concept only has a limited shelf-life and there remain many obstacles to be overcome if it is to be realised. For example, at the national level few defence planners have the necessary procurement expertise, properly trained and motivated. Allies have also in the past tended to use the future as an excuse not to engage the present. SACEUR's "family of plans", Defence and Deterrence in the Euro-Atlantic Area (DDA), and the Regional Defence Plans are all vital, but "what SACEUR needs tonight" must also be a priority.

62. All the above depends on the political and military cohesion of the Alliance. Indeed, cohesion is THE critical factor in the DDA because only then will deterrence be credible and if that fails defence be possible. Command and control is at the coalface between effective deterrence and defence. Credibility of such command-and-control systems and structures will only be assured if Allies and Partners step up to meet identified requirements because only then will C2 maintain speed of relevance.

63. Beyond 2035, tomorrow in defence planning terms, the emergence of hyperwar will demand speed of action as the essential partner of robust cohesion, speed of recognition, speed of decision and speed of assembly. Cohesion and speed must in turn be underpinned by interoperability of forces at the high-end of conflict, not only during peacetime exercises but when they are under extreme command duress. In such circumstances, assured speed will depend on the depth of force integration both combined and joint.

64. Any such force will, in turn, depend first and foremost on the quality and reach of sensors and communications as well as rapid analysis across the broad compass of the Alliance. If there is one critical change of command culture needed it is the development of cohesion-driven Alliance-wide, Partner-plus culture of automaticity of response. This is because "everything we do will be in a multinational environment, but at the moment we cannot even speak securely to each other". Given that future multi-domain operations will take place across land, air, sea, cyber, and space it is vital these domains are digitally and securely linked. They are not.

65. The corporate sector will also need to be incorporated into secure command nets. Between now and 2035 effective, increasingly hyper-fast ISR will thus be pivotal for both credibility and effect by providing “continuous observation” across both the analogue and digital dimensions of the battlespace and much of that system of systems will depend on autonomous technology. Such a concept is greatly hampered by the lack of trust that exists amongst Allies and Partners and their willingness to share all mission critical intel with each other. For example, the integration of human and signals intelligence remains imperfect. Moreover, ISR and military mobility will be increasingly dependent on access to the commercial sector and its systems, most notably heavy equipment transport.

Technology, Strategy and Future War

“We need to think asymmetrically as well as strategically”.

66. The overarching priority will be the establishment of architecture for the effective application and use of technology in situation sensing and situational awareness, and the development in parallel of cognitive advantage and predictive trends. However, it will be equally important to separate techno-fiction from science-fact and to think asymmetrically as well as strategically and to give the defensive as much due consideration as the offensive. This is because of need to by-pass adversary technologies through innovative and often asymmetric application of capabilities will be critically important and will thus place a particular emphasis on asymmetric solutions to technology challenges. For example, technologies often generate unexpected benefits, such as the use of autonomous underwater drones to enhance underwater critical infrastructure protection.

67. Agile minds will be as important as robust and adaptive command and control. This will, in turn, place a particular importance on updated professional military education (PME) that also makes best practice use of emerging technologies. Multi-domain operations will require an important emphasis on the need for constantly updated mission command culture supported by lifelong and distant learning, simulation, and advanced cognitive training.

68. “The aim must be that any shooter at any time is ready to engage”. Equally, all new technologies traverse through a “hype cycle” in which early over-expectation of performance gives way to over-cynicism before a plateau of realism follows. To avoid such a cycle the early establishment of expectation criteria would include, inter alia, the ability to properly assess “weak-tech” signals. Weak signals are past or current developments or issues with ambiguous interpretations of their origin, meaning or implications. They also include identifying research underway, often small in scale, which could lead to the next big tech breakthrough.

69. China is ruthless in the way it exploits Western universities in search of such technologies. The Allies need to become far more effective in countering these effort but also re-establish research links with academia. This is because Western academia too often seems to treat Chinese money with less suspicion than legitimate Western defence needs. A conscious effort needs to be made to change that. Universities are where unclear observables that warn about future trends and events take place and which the Alliance has traditionally found hard to exploit. The most obvious example of this dangerous paradox is China’s interest in biotech for good and ill, demanding of the West a response that is proportionate.

70. The Alliance also needs to exploit open-source Intelligence (OSINT) and proprietary commercial intelligence through a much more systemic and granular relationship with the broad commercial tech sector. Such a mature relationship would help enable technologies to be assessed more quickly and effectively for their military utility. Any such relationship will be vital so that AI, big data, machine-learning and autonomous systems etc. are not considered in isolation but rather as components of future

technology fusions, i.e., a Digital Dreadnought. This is also because such technologies are necessarily sub-sets of mutual supporting technology.

71. Conceptualising the place of new technologies in future force concepts should be first and foremost considered from the outset as human enablers and in so doing should place human beings front and centre. Where technologies do offer the prospect of a revolutionary “Digital Dreadnought” breakthrough in warfare, such as synthetic biology, they need to be very carefully and rigorously assessed. Indeed, how to quantify technologies in relation to effect and affordability will be critical to avoid expensive technology dead ends.

72. The Western Way of War will also need to balance offensive power, the application of EDTs and ethical constraint if future war democratic deterrence and defence is to be legitimate, credible, and humane. Consequently, the exploitation of technology in support of soft power will be as important as those applied in support of hard power. For example, technology will not only be central to dealing with the consequences of climate change but also enable the warfighter to operate in extreme environments.

73. The nature and scope of the Western Way of War will also see new actors engage with the state across the conflict spectrum, including the use of high-level destructive force and resource. There will be a range of such actors, but they will need to operate within clearly established rules of the game. Private military contractors (PMCs) will become increasingly influential warfighters. The Wagner Group was a significant factor in Ukraine and elsewhere, revealing both the utility and dangers should actors provide support for and against the state. PMCs follow corporate rather than national goals even though they provide crucial capabilities.

74. Powerful multinational civilian corporations, such as Starlink (Elon Musk), Amazon and Google, all of which have been active in Ukraine and have afforded Kyiv a technology edge over the Russians, which destroyed Moscow’s assumptions about the war. If not carefully managed the role of corporations in warfare could see a changing balance of power between the state and the corporate sector, not least because it is the corporate sector that is driving forward many of the critical future technologies with warfighting applications.

75. Private individuals are also increasingly influential in warfare, particularly with regard to funding. Individual citizens are becoming more engaged in geopolitics in increasingly anarchic democratic societies in which social media diffuses traditional loyalties. Crowdfunding, PayPal, and a host of other payment platforms have been used, for example, to help Ukraine buy drones which have devastated Russian land formations. Private groups are also helping to recruit individuals, hack critical systems, and undertake analysis. The democracies could be particularly vulnerable if such efforts were turned against them.

Technology Before Flesh

“NATO must avoid the tech paralysis of ethical analysis”.

76. Whilst emerging and disruptive technologies may not be the panacea for a new Western Way of War with its echoes of the ‘steel before flesh’ debates of World War Two, it is equally important to emphasise the utility of emerging and disruptive technologies on the continuities of war as it is to stress futuristic discontinuities and with it the judgement needed to understand this vital distinction. What will be particularly interesting over the next decade will be the extent to which the Allies and Partners together grip the interaction between old and new. Whilst there is as much a tendency to over-sell as under-sell the future of war, the Western Way of War WILL continue to place technology before flesh.

77. NATO must avoid the tech paralysis of ethical analysis. It is only possible to determine the properties of a system based on the properties any such system possesses. The argument over the scope and character of future war too often comes down to an undetermined and ill-defined belief in the democracies over what technology MIGHT achieve coupled to ethical concerns that follow soon after about what such 'tech' could lead to. Although some such systems are close to deployment in the civilian sector it will be some time before such judgements can be made. The danger for the democracies is that autocratic powers, such as China and Russia, have no such concerns and will simply seek to exploit such technologies for narrow strategic advantage. The focus of democratic leaders on human security rather than territorial integrity could also gift the edge to the autocracies forcing the former to react rather than lead. This means the very process of statecraft will need to be accelerated if sound judgements are to be made quickly.

78. Change is clearly afoot even if much of the discourse about future war is really about the here and now. Therefore, a conscious balance must be struck between planning and blind futurism because all such predictions are based on assumptions that could easily change. Rather, the focus should be on what is known and how to empower the here and now to generate deterrence and defence effect. This is because it is easier to predict where wars might happen than how wars will be fought. Where are the obvious flashpoints? The Russo-Ukraine War has more in common with the trenches of World War One than some futuristic battlescape, albeit with the use of drones for surveillance.

79. Equally, there can be no room for complacency. The conference confirmed its core hypothesis – that technology will profoundly change the character of war between 2023 and 2050 and that those responsible for making decisions about what forces and resources to invest in defence suffer from an insufficient understanding of the nature, scope and application of technologies that together could make a difference not unlike the use of atomic weapons in 1945 or the launching of HMS Dreadnought in 1906.

80. There is a particular problem with strategists predicting tactics and tacticians employing strategy. Strategists get armies to war, tacticians fight it, but both need to understand the nature of the fight in which they are engaged, particularly enemy capabilities. If not, both strategists and tacticians are simply creating the conditions in which their forces will find themselves at the wrong end of a new form of Blitzkrieg.

81. Over recent years there has also been a tendency in Western countries to elevate strategy and demote tactics, which should be only ignored at their peril because there will be layers of warfare in which a complex interaction between tactics and technology will be the norm. Even quite 'primitive' actors such as Hamas exploit new technologies, some of it quite basic, for tactical advantage.

82. There is furthermore a pressing need for a much clearer distinction between the 'strategic' and the 'tactical'. For example, space-based systems are strategic because they are vital for protecting the backbone of all operations. Those systems which do not provide an architecture capability are thus by definition tactical.

83. Perhaps the most important finding of the conference is a truism that has long stood the test of time – preventing wars and fighting wars successfully is dependent on a host of vital partnerships. Partnerships between strategists, technicians, and academics, between scientists, technologists, and practitioners, between civilian and military, but above all between the public and private sectors as part of a strategic public private partnership. If technology is to be fully integrated across the civil-military security-defence-resilience paradigm much of the effort will need to focus on pan-effort doctrinal development so that technology can be applied comprehensively and evenly across force and resource.

84. Enthusiasm should also be tempered by realism as history is replete with examples of action being stymied by counteraction. Technology will also breed vulnerabilities as well as advantages and the Western Way of Future War, most notably hyperwar, will demand a systematic consideration of such weaknesses. There is already a glaring example of such a weakness. Hi-tech systems are reliant on critical raw materials and rare earth materials very few of which are controlled by the democracies, with many under the command of China and Russia. Ninety percent of high-end semi-conductors are made by the Taiwanese company TMC. At the very least, stockpiles will need to be built to ensure some degree of critical security.

The Western Way of Future War

"Those developing it (EDTs) have a vastly better understanding of its applications – good and ill – than those who will be responsible for applying it".

85. The Western War of Future War will see AI, machine learning, quantum computing, synthetic biology and other such EDTs front and centre in deterrence and defence, which will in turn become increasingly reliant on sensors and the revolution in speed and capacity underway. Sensors are at the core of future multi-domain warfare and much of the effort should be focused therein if the greatest return from the highest investment in the most useful technology is to be realised to the greatest effect.

86. At the same time, any Allied technological advance will see the adversary adapt, and one test will be the capacity to better understand how China, Russia and others will adapt to a changing character of Western warfare, as adapt they will. Moreover, Chinese collaboration with developing countries also suggests the transfer of advanced technologies will be faster and more widespread than many in the West believe.

87. In 2023, Elon Musk said: "AI labs and independent experts should pause to jointly develop and implement a set of shared safety protocols for advanced AI design and development that are rigorously audited and overseen by independent outside experts." This statement highlights a dangerous paradox at the core of the future war, strategy and technology paradigm – those developing it have a vastly better understanding of its applications – good and ill – than those who will be responsible for applying it.

88. Why are we not listening and stopping what might be a mad rush to oblivion? Eighty years ago, the development of atomic science led to both abundant energy and the first weapon of mass destruction. However, the lack of understanding in Western governments led to cynicism in power about breakthrough scientific and industrial innovation. The so-called precautionary principle emphasises caution before any potentially revolutionary technology is exploited. Western adversaries?

89. The hard truth is that Western governments have enshrined the precautionary principle into the 'not spending money' principle on the grounds that few 'fancy gadgets' ever work. This has stifled innovation and led to controversial decisions, such as the ban in some countries on genetic modification (GM) for reasons that are little more compelling than the burning of medieval witches.

90. Secretary-General Lord Robertson once rightly said it is all about "capabilities, capabilities, capabilities", but such capabilities cannot be generated until there is understanding, understanding, understanding! Sooner rather than later these days 'new' tech becomes old tech and inevitably spreads. AI, machine learning, quantum computing etc cannot be un-invented, and if the Western democracies do not exploit it other will. Make no mistake, the changing character of warfare is facing not just a set of force multipliers but immeasurable magnifiers.

91. The simple truth is that no-one really understands how AI will develop and few policymakers have the imagination to envision future war, particularly when AI is fused with other technologies to realise a Digital Dreadnought moment, or rather a fleet of Digital Dreadnoughts moment. Therefore, NATO, its Allies and Partners urgently need to commission a study by the Chief Scientist to precisely do that.

92. The last word is left to the Bletchley Declaration: “All actors have a role to play in ensuring the safety of AI: nations, international fora and other initiatives, companies, civil society, and academia will need to work together. Noting the importance of inclusive AI and bridging the digital divide, we reaffirm that international collaboration should endeavour to engage and involve a broad range of partners as appropriate, and welcome development-orientated approaches and policies that could help developing countries strengthen AI capacity building and leverage the enabling role of AI to support sustainable growth and address the development gap”.

Working Group Summaries

Technology Working Group

Headline: NATO should develop and share a high-level “grand strategy” to drive innovation and EDT adoption. The strategy should be comprehensive, from creating the conditions for a dynamic, responsive innovation ecosystem through the development process (identification, test, learn, refine, iterate, validate, scale) to delivery, adoption, and integration. This grand strategy should include the purpose of innovation and EDT adoption, the roles of NATO stakeholders and external players, and the ways and means to ensure dynamic, accelerated, and effective (interoperable, high impact) innovation and EDT adoption. An external and frank audit of how NATO currently facilitates innovation and EDT adoption with respect to NATO ambition may help identify key areas for improvement.

93. Adopt a systems approach to EDT capability integration (e.g., DOTMLPFI – doctrine, organization, training, material, leader development, personnel, facilities, interoperability), and life cycle management and sustainment, including in-life modernisation and obsolescence management. Improve the quality, depth, and breadth of dialogue with private sector players to leverage the full spectrum of private sector contributions to NATO innovation and EDT adoption. Communicate defence needs as discrete (but sufficiently broad) concepts of operation that would enable and leverage the private sector’s ability to creatively develop innovative approaches.

94. Focus innovation on those EDTs (or new applications of existing technologies) that add greatest value for NATO’s priority defence challenges, especially those that need military input and guidance and funding to respond to priority defence challenges. Follow through with full resourcing and refinement of NATO innovation initiatives (i.e., DIANA, NATO Innovation Fund) and accelerate and expand as possible to exploit their potential.

95. Adopt agile development and acquisition principles to accelerate development and delivery and improve opportunities to better leverage contributions from the private sector to address defence problems. Promote modularity, compatible digital backbones, and NATO standards. Revise NATO resource and capability development processes to improve agility, enable rapid iteration, allow for failure, and accelerate development and delivery.

96. Use market incentives and levers to promote defence-related research, development, testing (e.g., meritocratic competitions) and experimentation. Leverage all domain opportunities for operational experimentation. Improve adaptive, responsive military concept development to accelerate and improve adoption of maturing EDTs (i.e., concepts of employment, doctrine, and TTPs). Account for data and cyber security, supply chain security, climate change-related requirements (and others) in the NATO

innovation and EDT adoption processes.

97. Address technological literacy among policy makers, decision makers, resource managers, and operators. Consider adaptive adult learning, scenario-based experiences, and simulations to provide high-impact training and education to leaders with limited time. NATO Digital Transformation will advance interoperability in data, connectivity, and networks and should be implemented rapidly as a foundational enabler for EDT adoption. Likewise, NATO's Multi Domain Operations Concept and Implementation Strategy will be drivers for interoperability requirements (see Warfighting Development Imperatives).

Military Strategy and Future Force Working Group

Headline: There is insufficient urgency in relation to the risks of not leveraging sufficiently, and on an organised basis, the benefits of new technologies for strengthening the

combined operational capacity and political unity of the Allies. This greater sense of urgency should lead to adopting an "end-to-end" approach to technological innovation and transformation among the Allies and across the Alliance; this comprehensive approach should incorporate political, institutional, procedural, operational and industrial dimensions, possibly starting at the forthcoming 75th NATO anniversary summit in Washington, D.C., in July 2024.

98. A deliberate and comprehensive approach to technology should be driven by the concept of "participatory enterprise". This is where national governments, international organisations, and industry, including technological startups, enter a compact to structure and accelerate the transformation of defence and security and be prepared to address with civil society the potential risks and constraints associated with increased technological dependencies, from the standpoint of national security policy, civil-military relations and ethics.

99. As this report makes clear, while the forthcoming technological revolution brings military risks as well as opportunities for the Allies, it also requires a broader, more holistic, more imaginative, and more innovative approach to defence policymaking and defence organisation. This means that alongside the forthcoming technological revolution, defence establishments and the armed forces must initiate and manage competently a conceptual revolution of possibly unprecedented complexity and consequence.

Capabilities Working Group

Headline: The strategic environment we will face in 2035 will be bleak. Taken together, the nature of the 2035 threat will likely be high-tech, industrialised and protracted, and will require whole of government, fully mobilised, resilient, national responses, including incentivising industry for surge capacity and protracted production. The budgets generated to finance these must be affordable. However, they will require further increases – there is no peace dividend now in sight.

100. No one nation will be able to respond adequately to address this wide spectrum of threats alone. Responses will need to be founded on cooperation and integration of Allied and like-minded Partner nations, both in the NATO and Indo-Pacific regions (emerging examples will include AUKUS and other regional groupings such as the UK Joint Expeditionary Force (JEF)). This will require cultural change, including more technology transfer, interoperability, standardisation, joint procurement, logistics and sustainment.

101. The biggest risk Allied and Partner countries face is time. They will lose their already tenuous competitive advantage against threats if they fail to make the necessary bold adaptations, which include optimising political and military cooperation frameworks to integrate new EDTs at pace in multi-domain concepts at scale (for example: the Replicator and DIANA initiatives and the NIF and emerging JEF capabilities funding mechanisms).

102. An advantage exists: the recognition that this is a moment not experienced for some time, which if seized can put advanced democracies in a position to field capabilities in 2035 that will remain functional until 2060 in some cases. This advantage, then, is the collective 'Western' unity of purpose against the distinct but increasingly aligned State threats we face. This provides the opportunity for accelerated adaptation and learning through pragmatic change management, which in turn requires vision and top-down leadership empowered by clear guidance from statesmen.

103. This also means our capability strategies and approaches must be adapted and accelerated, our adoption of tech and integration processes must be focused on generating speed while ensuring effective testing, experimentation and demonstration. This will require closer partnerships with industry to adapt and adopt new acquisition and sourcing processes. Nonetheless, we must also maintain the established processes that work and sustain our legacy systems while seeking out new methodologies (with industry advice) to do this. The NATO Defense Planning Process (NDPP) plays a necessary role. But it must be complemented by vanguard groupings under lead nations that can and will go faster if provided with innovative investment funding mechanisms.

104. What does this mean for capabilities? The emerging and disruptive technologies such as AI, quantum, big data, improved processes in digital sourcing et al, will need to complement and improve legacy capabilities, but they will also enable key new capability categories.

Strategy and Policy Working Group

Headline: By 2035, there well could be a NATO 4.0 adaptation, shaped not just by geopolitical change but a revolution in military technology beginning in this decade that changes the very character of warfare. There is also the possibility that instead of a NATO 4.0 driving military technology in 2035, NATO will remain at the outdated version 3.0 because the Allies did not move fast enough to stay on the leading edge of technology. NATO's adversaries may have made a different decision.

105. NATO in 2035 could see the US still in a leadership role but with reduced engagement in NATO, for political reason or because the US is occupied in another theatre, like the Indo-Pacific. If current defence spending trajectories hold, the European pillar at NATO, including Ukraine, may have the capability and willingness to take on more responsibility and fill gaps left by US forces being used elsewhere. But filling those gaps seamlessly will be critical, as the Russian threat to European stability will likely have increased. By 2035, a seething Russia could be in the middle of rebuilding a more professional and capable military guided by lessons from the war in Ukraine, including incorporating modern military technology. A hostile China will likely be seen by NATO as more of a threat than it does today, continuing unabated its military build-up and harnessing new military technology.

Industrial Implications and Procurement Working Group

Headline: It is not enough that our leaders are seeking to understand new technologies - that is only the first step - they must assign time and effort and make it their business to reform the policies that add friction to innovation pull through, shorten the processes, better align incentives, and create a culture that embraces risk in a different way.

106. Effective adoption of new technology will provide a strategic advantage over our enemies which can improve both deterrence and the chance of victory in combat. This edge is best defined today by two overarching functions: 1) Increased speed of the understand-decide-act cycle, leading to an accelerated tempo of operations and 2) Increased lethality through increasingly smart autonomous systems. Both functions are, ultimately, the result of innovations in software but is all for nought without effective adoption and bringing new technology to bear on the mission.

107. Governments have an innovation adoption problem, not an innovation problem per se. Therefore, if the democracies are to be serious about fixing this challenge, leadership at the highest level must focus on fixing the adoption process with clear accountability for pulling through new technologies from research to production. There are excellent examples of innovation adoption models in the Alliance. We should be thinking of Picasso; good artists borrow, great artists steal. Nations should steal these great examples; don't reinvent the wheel! The private sector will continue to be the beating heart of innovation (70% of all research and development comes out of the private sector) due to economics and talent. Commercial innovation will continue to accelerate as AI increases the productivity of industries and the effective adoption of dual use technologies will increasingly become essential to delivery of cutting-edge capabilities.

Training and Leader Education Working Group

Headline: Defence and security institutions need a more accessible, continuous, personalized, and adaptable learning culture to gain and sustain an intellectual edge over competitors and adversaries.

108. Defence and security institutions need a more accessible, continuous, personalised, and adaptable learning culture to gain and sustain an intellectual edge over competitors and adversaries. Training and Leadership Education is crucial for the competitiveness of the Alliance. Professional development in defence and security should consider the concept of a "Total Defence" scenario in a poly-crisis and comprise 4 main categories: 1) Command leadership and ethics, 2) Joint warfighting/multidomain war fighting, 3) Strategy and Policy, and 4) Technology and capability.

109. Institutions in defence and security should define and clearly communicate what they require in terms of skills, knowledge, and experience at all ranks/grades (and, preferably, by individual posts). They should properly resource the learning and professional development process with time, money, and personnel. The institutional leaders – at the time - must own the whole process and advocate for it on behalf of their institutions (stewardship).

110. The equivalent of 2.5 % of national security and defence budgets should go to professional development, including education and leadership development [this figure is analogous to UK national target for expenditure on R&D]. The 2.5 % for professional development should be counted towards each country's contribution to meeting the NATO commitment to spend at least 2% of GDP on defence.

Ethics and Legal Working Group

Headline: NATO has good reasons to agree and promote ethical norms and guidelines about the military uses of new technologies. However, the present prospect of winning consent from Russia, China, and the Global South to new international law is not promising.

111. While seeing what can be done to create diplomatic common ground for a new international treaty, and considering how the new technologies might enhance its own compliance with current International Humanitarian Law, NATO should also focus on strengthening agreement on norms among its member-states and using its market-power and liaison with professional bodies to promote them worldwide. In addition, it should support the relevant education of senior decision-makers.

The Dreadnought Working Group

Headline: NATO and allies should recognize that strategic shock often arises from incorrect intelligence assessment and therefore improve intelligence sharing and assessment among individual allies (not NATO collectively) – this is possible when there is a shared interest. There should be greater red teaming of assessments by using AI/computing.

112. Enhance resilience using Total Defence concepts, fulfilling NATO's baseline requirements on resilience, and ensuring alignment with the NDPP. The risk of unrest/uprisings as reactions to potential use of nuclear weapons should be addressed by engaging civil society. Start considering asymmetric responses – creating unexpected combinations of responses with difficulty of attribution, massive cyber-attacks, attacks on satellite systems, hitting for instance internet, banking, food and water supplies, and create our own Dreadnought moment.

113. Ensure flexible response options. For the military, long range delivery systems, conventional and or nuclear, are needed. Nuclear weapons are our strongest response and that instrument needs to work better to be credible. An interesting conclusion is that new technology is just one element that is necessary for military strategy. Rather, technology needs to be seen as part of a broader civil/military system if it is to be decisive. As with nuclear weapons, EDT combinations could indeed help deliver strategic military shock, but they need to be incorporated into a wider system to be effective.

Appendices

Conference Programme

MONDAY 9 OCTOBER

1300 Participants arrive and buffet lunch available – informal dress.

1500-1515 Welcome and Mission Statement

General the Lord Richards of Herstmonceux, Former Chief of Defence Staff, UK; and Conference President (The Alphen Group)

Dr Robert Grant, Programme Director, Wilton Park

Professor Julian Lindley-French, Chairman, The Alphen Group and Conference Director

1515-1545 Keynote: The Future War, Technology and Strategy Challenge

General Chris Badia, Deputy Supreme Allied Commander Transformation, Allied Command Transformation, Norfolk

1545-1630 Session 1: Future war, strategy and technology 2043 – trends

This plenary session will frame the work of the conference and the working groups by looking out to 2043 and offering a vision of future war and the likely role of technology in fighting it. This discussion will draw on relevant lessons from the war in Ukraine and consider the requirements for democratic armed forces.

Lessons from Ukraine
Maj Gen (Ret) Mick Ryan, Mick Ryan Leadership; former Australian Army Major General

Technology trends
Dr Bryan Wells, Chief Scientist, NATO

Requirements for democratic armed forces
Dr Ulrike Franke, Senior Fellow, European Council on Foreign Relations

A vision of future war
Professor Sir Lawrence Freedman, Emiritus Professor of War Studies, King's College London

1630-1700 Tea/coffee

1700-1900 Session 2: Future war, strategy and technology 2043: world café format discussions

The four speakers from session one will each chair a world café discussion on their above topic. In this format, participants will divide into four groups and spend 25 minutes in each world café room before rotating to the next. The same chair and rapporteur for each room/topic will remain in place throughout the session.

1900 Reception followed by dinner with speakers from industry sponsors

TUESDAY 10 OCTOBER

0800-0845 Breakfast – formal civilian dress

0900-1030 Session 3: Exploiting science and technology: briefings

Briefing 1: Artificial Intelligence, Autonomy, Big Data, and Information and Communication Technologies (Julian Lindley-French)

Briefing 2: Synthetic Biology and Human Enhancement (Julian Lindley-French)

Briefing 3: Space-based capabilities, Novel Materials, Energy, and Hypersonic Systems (Rob de Wijk)

1030-1115 Photograph followed by tea/coffee

1115-1245 Session 4: Key enablers: briefings

Briefing 1: Cyber Future War including Information Warfare and Ubiquitous Communications (Madeleine Carr)

Briefing 2: Future Architecture, Command and Control in Hyperwar and Future ISR – from Sea-bed to Space across the Multi-Domain Battlespace (Ben Hodges)

Briefing 3: Mission Command and the Cognitive Dimension (Ben Hodges)

1245-1345 Lunch (including working lunch for chairs and co-chairs of working groups with Lead Group to confirm respective missions and method – Conference Room)

1345-1445 Session 5: Sponsor show and tell: WHO ARE YOU AND WHAT DO YOU DO?

1445-1615 Session 6: Working Group Session One

Working groups session one – mission, work plan & opening discussions (Groups will remain the same throughout the 4 working group sessions).

Group 1: Technology Working Group

Group 2: Military Strategy and Future Force Working Group

Group 3: Capabilities Working Group

Group 4: Industrial Implications and Procurement Working Group

Group 5: Strategy and Policy Working Group

Group 6: Ethics and Legal Working Group

Group 7: Training and Leader Education Working Group

Group 8: Dreadnought (Technology & Strategy Fusion) Working Group

1615-1645 Tea/coffee

1645-1815 Session 7: Working Group Session Two: Discussions

1815-1845 Free time

1900 Reception followed by formal civilian attire conference dinner hosted by General the Lord Richards of Herstmonceux with keynote addresses by General Sir Patrick Sanders, Chief of the British General Staff and Professor James Holland

WEDNESDAY 11 OCTOBER

0800-0845 Breakfast – informal dress.

0900-1030 Session 8: Working Group Session Three: Discussions

1030-1100 Tea/coffee

1100-1230 Session 9: Working Group Session Four: Preparing Report Back to Plenary

1230-1330 Lunch

1330-1500 Session 10: Working groups report to plenary and follow on discussion of linkages between working group themes

During this plenary session the working group chairs and co-chairs will report back to conference with the main findings of their respective teams. Each Working Group will have up to 7 mins to present their respective main findings with 5 mins allowed thereafter for clarifications to plenary.

1500-1510 Session 11: Evaluation survey

Completion of online survey

1510-1540 Tea/coffee

1540-1600 Keynote: The Future War, Technology, Strategy, and Innovation: The Way Ahead

Air Chief Marshal (Ret) the Lord Peach, former Chief of the British Defence Staff and Chairman of the NATO Military Committee

1600-1700 Session 12: Future War, Strategy and Technology – the way ahead and final remarks

This plenary session will close the conference with a discussion of the way ahead – both next steps and looking further forward. What are the key takeaways from the conference plenary session and working group deliberations? The session will also consider the possibility of follow-on work emerging directly from the conference.

1900 Informal dinner

THURSDAY 12 OCTOBER

0800-0845 Breakfast and checkout – informal dress.

0900 Participants depart

Full working group findings and recommendations

Working Group 1: The Technology Working Group

Chair: **Dr Camille Grand (France),** former NATO ASG for Defence Investment (TAG)

Co-Chair/Rapporteur: MG (Ret.) Gordon B. Davis (US), former DASG NATO Defence Investment Division **(TAG)**

The Technology Working Group considered the future applications of emerging and disruptive technologies in the battlespace across all domains from sea-bed to space, Emerging and disruptive technologies include artificial intelligence (AI), autonomous systems (including drone swarms), big data, information and communication technologies (ICT), energy and propulsion technologies, hypersonic systems, electronic and electromagnetic technologies, space-based capabilities, and the future role of quantum technologies (computing, communications, sensing), novel materials and advanced manufacturing, and biotechnology and human enhancement. How are these technologies changing current warfare (e.g., in Ukraine, Nagorno-Karabakh, Libya...) and how will they affect future warfare? What impact these technologies have on the OODA loop – observe, orient, respond, act? What technologies might be most useful in maintaining the West's comparative military advantage? For deterrence and defence and / or resilience? What mix of technologies will be the exclusive domain of a few nations (friendly and foe) and which will be available to all, with what implications for the Alliance, EU, and partner future forces? What decisions must be taken now to ensure research and development, testing and experimentation of advanced technologies to ensure their availability and fielding by 2035? What new defence concepts systems and military techniques, tactics, and procedures must be developed in tandem with fielding of advanced technologies to ensure their optimal effect (deterrence and defence, resilience)? What policies and mechanisms will be needed to preserve interoperability among NATO allies, EU member states and partner future forces?

Elizabeth Buchanan (Australia), Head of Research, Royal Australian Navy

Madeleine Carr (UK), Professor in Global Politics and Cyber Security, Director of the Digital Technologies Policy Laboratory, University College London

Nancy Pallares, (US) Business Development Director, Teledyne Europe

Tristam Constant (UK), Director, Europe, Anduril

Chris Moore-Bick (UK), Policy Head, Defence Science and Technology, Ministry of Defence

Giles Hill (UK), Former Assistant Chief of Defence Staff and Deputy NATO Coalition Commander

René Balletta (UK), First Sea Lord's Visiting Fellow, Royal United Services Institute (RUSI)

Ulrike Franke (France), Senior Fellow, European Council on Foreign Relations

THE REPORT

Under the Chair of Camille Grand and Co-Chair Major General (Retired) Gordon "Skip" Davis, the Technology Working Group considered the future applications of emerging and disruptive technologies in the battlespace, implications for NATO (applicable for the EU as well), and how best to adopt and integrate them for comparative advantage. The group included members with NATO, government, defence, and private sector experience and expertise. Following a review of the core messages and themes of our discussion, we summarize the most important findings and recommendations in this report.

Core messages

NATO's current list of emerging and disruptive technologies that should be promoted for development, adoption, and protection to gain and maintain a technological edge vis-à-vis potential adversaries and challengers *is about right*. NATO has arrived at their current list

iteratively through a process of research, internal debate, and policy development. The group discussed various aspects of technology maturity, impact on defence and security, and interdependency, concluding that the NATO list was sound and well founded.

NATO needs a high-level, comprehensive "grand strategy" for the technological domain to ensure innovation and EDT adoption lead to the technological edge NATO aims to achieve. *NATO processes* related to innovation and EDT adoption *need further refinement or revision.*

NATO efforts in innovation and EDT adoption should focus on NATO's mission, roles, and added value to its members. NATO's mission and core tasks (especially collective defence and deterrence and conflict prevention and management) plus resilience should drive the selection of defence challenges needing solutions through innovation and EDT. *NATO should leverage its roles* as a facilitator, integrator, organiser, norm and standard setter, developer of common doctrine, common concepts and policy, and driver of collective defence planning *to guide innovation and EDT adoption.*

At best *NATO can aspire to be an early adopter and norm setter but it will always be a limited driver* of EDT development and acquisition due to the limited common funds NATO invests and the limited demand for collective capabilities (products and services) NATO represents.

Main themes of the debate

The purpose of NATO innovation and EDT adoption is important to maintain as a compass for prioritisation of effort. Our group concluded that this purpose is to help NATO secure and defend the Alliance (nations, populations, forces), deter aggression, mitigate challenges, prevent and manage conflict, and increase and sustain resilience.

Should NATO prioritise its efforts on selected EDTs? If so, how? There was a general view that NATO needed to prioritise its EDT efforts. However, after a review of NATO's current list of priority EDTs and potential criteria, the group agreed that NATO's current approach of focusing first on developing strategies and policies for *EDTs that are foundational or common components of key combinations of EDTs* (e.g., Artificial Intelligence, Big Data, Information & Communication Technologies, Autonomy, Space) made sense. Additionally, those *EDTs that are mature now or likely to mature by 2035* should be prioritised for development strategies (and military concept development) to assist NATO and nations in incorporating EDT-related capabilities in the next two NATO Defence Planning Process (NDPP) cycles (i.e., 2023-2026, 2027-2030). Given that the majority of NDPP national capability targets fall in the near-term (0-6 years) a horizon of 2035 is appropriate (i.e., the apportionment year of the next NDDP cycle is 2029; 2035 is 6 years beyond).

Are there combinations of EDTs that may be having or could have a high-level, game-changing impact (i.e., incite a Revolution in Military Affairs - RMA)? The group believed one combination was having a RMA-level impact now: AI, Big Data and Information and Communications Technologies (ICT), Autonomy, and Space-related capabilities. The group also identified two combinations of EDTs that could have a RMA level impact in the future: 1) AI, Big Data and ICT, Quantum Technology, and Space-related capabilities, and 2) AI, Big Data and ICT, and Biotechnology and Human Enhancement.

Where should NATO follow, partner, or lead in defence-related innovation? Based on what criteria should NATO take a leading role? The group discussed when government or military Research and Development (R&D) should fund innovation versus follow private sector lead. The group also discussed where governments and militaries might have the preponderance of expertise in EDT development (e.g., hypersonic systems).

The issue of *quantity versus quality in select EDTs (such as autonomous systems and satellites)* is important for NATO to consider. Governments may be content to depend on the private sector for large numbers of relatively cheaper systems while focusing military development on small numbers of more costly, hardened, and exquisite systems with military-specific capabilities. *Determining the right mix* of innovative technologies to invest in for defence capabilities will be important. For example, commercial of the shelf (COTS) drones

that are cheap with limited survivability, but which provide tactical advantage (e.g., ISR, targeting, strike) when employed in mass should complement higher quality drones which are limited in number with military-specific performance characteristics (greater survivability, exquisite sensors or munitions) and acquired at greater cost. That said, traditional trade-off relationships are evolving - high versus low tech, quality versus quantity, high cost versus low cost, available later versus ready now.

Leader education is a critical aspect to investing in innovation and EDT adoption. Informing, educating, and translating the importance of EDTs to non-expert policymakers and decision-makers (politicians, diplomats, military leaders, and resource managers) is essential to securing investment and support for the conditions needed to promote innovation and EDT adoption**.**

Interoperability (material and operational, a greater problem for material) is a current shortfall. Interoperability is driven by military requirements and shaped by doctrine and concepts of employment. *What is right level of system interoperability?* The answer may be domain specific. As physical domains are each distinct the level of system interoperability is driven by how national forces organise and fight under NATO command. Cyber and space interoperability are driven by the needs for data-centric connectivity and what resources are retained by nations versus offered to NATO to achieve specific collective effects. Given these distinctions, how should NATO inform industry of interoperability requirements and the related context to guide EDT development and delivery?

NATO and national innovation ecosystems are key to accelerated development and delivery. There are multiple NATO innovation stakeholders (Nations, NATO Committees, S&T Organisation, International Staff, International Military Staff, Strategic Commands, Agencies, DIANA, NATO Investment Fund, Industry) each with different agendas and priorities. NATO and national innovation ecosystems are not naturally coherent and need to be enabled with common aims, priorities, and processes.

Diversity and variety (as opposed to common systems and equipment) contribute a quality of their own. While diversity and variety may challenge interoperability and complicate adopting common standards, they can be helpful in posing tactical (and perhaps operational or strategic) dilemmas for adversaries. NATO and nations should consider which EDTs will be exclusive to a few countries (e.g., hypersonic and counter-hypersonic systems, space-related capabilities) and which EDTs may be available to all. Those EDTs exclusive to just a few countries may not be worth extensive NATO effort.

Cost of EDT development and adoption is a major factor for NATO and nations. *Predictable funding is key for industry*. Increased defence investment often requires domestic spending and / or internal defence budget trade-offs. When considering EDT investment and adoption we can't forget the need to enhance and / or recycle legacy capabilities and to enable life cycle management & sustainment (including obsolescence management) to leverage past investments in a cost-conscious manner.

Not all domains are the same in terms of EDT innovation and adoption. Some EDTs such as AI, Big Data and ICT, Autonomy, Quantum Technology, or Biotechnology and Human Enhancement may have common aspects across the physical domains. Cyber and space, however, are enablers for each other and the physical domains while also being operational domains of their own accord. As such cyber and space are common enablers for all NATO EDTs and should be considered in EDT innovation and adoption (including in policy, capability strategy, concept, and standards development).

Obstacles to delivery

The group identified several existing and potential obstacles to innovation, and to development, delivery, and adoption / integration of EDTs.

There is limited understanding among high-level leaders (policymakers, decision makers) and resource managers of EDT potential and the need to accelerate development and delivery to seize opportunities for gain and avoid the costs of delay or non-adoption. High-level leaders generally have a limited time available to learn and a limited attention span due to competing priorities.

The way we train and educate leaders and staff and recruit and retain EDT-related expertise is sub-optimal.

The way we organize for innovation and EDT adoption (including the way we procure EDTs) is not fit for purpose.

The lack of a systems approach to EDT adoption and integration (at political and policy level) inhibits NATO's and nations' ability to leverage EDT potential.

Budget constraints (funds available, past decisions, rigid and long budget cycles, industrial policies) impact the level and consistency of defence investment for R&D and procurement from industry.

NATO resource processes and the common fund governance (resource committees, common funded capability development process) limits the effectiveness of NATO investment.

Unpredictable, inconsistent, or insufficient funding constrains the ability of startups and Small and Medium Enterprises (SMEs) to contribute to defence-related EDT development. Short term return on investment generally drives large industry. This behaviour can starve SMEs and startups who need longer term investment to develop and mature EDT.

Lack of robust, continual, mutually-beneficial dialogue between all levels of defence-relevant industry and military limits mutual understanding of defence challenges and potential private sector solutions.

The complexity of the NATO innovation ecosystem complicates internal coherence and external engagement. Information sharing of defence strategies, capability development approaches, and defence challenges with the private sector is limited and insufficiently transparent.

Lack of speed and risk tolerance in defence procurement leads to loss of opportunities.

Lack of doctrine and employment concepts limits speed and effectiveness of EDT adoption and integration.

Export licensing and technology sharing constraints can limit multinational cooperation in EDT development / acquisition and delivery and thus adoption.

National desire to retain control of and a limited willingness to share exquisite capabilities (e.g., cyber, space, niche capabilities – hypersonic systems) can limit EDT exploitation / adoption.

Technological immaturity limits speed of adoption and ability to develop concepts of employment, thus limiting the immediate relevance and desirability from an end-user perspective.

Cyber security is a vulnerability throughout innovation and EDT adoption.

Supply chain security for critical components and resources needed for EDT development, production, adoption (e.g., information technology, rare earth materials) can limit EDT adoption at scale as well as life cycle management and sustainment.

Specific Working Group findings

The private sector dominates R&D funding and effort in EDT and in EDT expertise. *NATO should follow private sector lead where* commercial and private research and development funding dominate EDT development and EDT characteristics largely address military requirements (i.e., most areas of dual-use technology and applications). *NATO should partner*

where private sector EDT development needs additional scope and focus to address defence challenges. *NATO should lead where* private sector EDT does or will not address defence challenges without specific military funding (e.g., hypersonic weapon systems).

Potential criteria for NATO EDT prioritisation: mature technology (high Technology Readiness Level), *high impact and high applicability to defence and security needs* (responsive to known challenges / vulnerabilities), *enabler of Multi Domain Operations and Warfare Development Agenda, enabler for drastic improvement of legacy systems, foundational, cost-effective. NATO focus should remain on high-impact, game-changing EDT combinations with military application* (i.e., which address greatest defence challenges).

Quantum Technology development will present future challenges that need to be addressed now, e.g., quantum-proof encryption and countermeasures for quantum-sensing (e.g., greater uncrewed autonomous systems, mobile Faraday-type protection).

Importance of Digital Transformation (e.g., people, processes, technology aspects – data fabric, connectivity and networks, standards – digital backbone for systems) as an underlying enabler for EDT adoption and addressing complex interoperability problems.

Importance of adopting a software-centric approach and component modularity wherever applicable to enable faster upgrade, iterative improvement and refinement in response to new technologies, new applications, and response to adversarial action or adversarial reaction.

Importance of cyber security throughout innovation and EDT adoption. Cyber security concerns extend to private sector collaboration (from R&D to testing and experimentation to delivery), especially to protect classified or sensitive defence information (including intellectual property). Cyber vulnerabilities can emerge during adoption and integration as operators employ EDT. Cyber security must be embedded in a holistic systems approach to integration (including training and education of operators, maintainers, leaders).

Private sector has difficulty in understanding how and where to engage NATO on innovation due to the complexity of the NATO enterprise.

Within private sector large industries (traditional and non-traditional), SMEs, and startups can all potentially contribute to defence challenges and have different comparative advantages and information/funding needs. SMEs and startups tend to lead on software, cyber, data, simulations expertise.

Private sector responds to market incentives and levers and regulation. In addition to technology transfer, national and international regulation will likely drive “Net Zero” climate impact compliance and supply chain security considerations (e.g., re-shoring, friend-shoring, decoupling from autocratic regimes).

Importance of adopting an accelerated development cycle - test, learn, refine, scale – to leverage potential of EDTs in timely manner (to maintain NATO’s comparative advantage against innovating adversaries).

Identification, refinement, resourcing / financing, and adoption of EDT requires a multi-stakeholder approach (scientists & engineers, military, armaments, industry, resource / budget managers).

*Accelerated development and delivery require accelerated procurement and acquisition processes, and higher risk or failure tolerance***.**

NATO provides added value in operational experimentation and should expand opportunities for bringing key innovation players together (i.e., bring operators/commanders, industry developers, scientists & engineers together to refine requirements, validate and refine prototypes, identify the need for new doctrine, concepts, and tactics, techniques, and procedures, and then validate them).

Importance of a holistic, systems approach to EDT capability integration. NATO and NATO nations already use a comprehensive approach to new capability integration (i.e., consider aspects of Doctrine, Organisation, Training, Materiel, Leader Development, Personnel, Facilities, Interoperability – DOTMLFPI). Systems engineers and capability integrators with cross-organizational views and authorities are needed to implement EDT-related change effectively. Some governments and industry use Chief Technology Officers to help integrate EDT-related capabilities. Perhaps NATO could identify a CTO for the NATO enterprise.

Multinational cooperation is important for most nations to acquire affordable technology at speed. NATO offers opportunities for multinational cooperation in EDT-related capability development and procurement.

NATO as Adopter (capital A for emphasis) versus driver of EDT. NATO's greatest added value to nations is in promoting and facilitating defence-related innovation and EDT adoption. Because of its limited resources, NATO is more of an Adopter of relevant EDT than a driver of EDT development and delivery. NATO Adopter roles include forum for collective prioritisation; organiser and integrator of capabilities and forces; facilitator for policy, doctrine and concept development; standards and norms developer. NATO driver roles include leveraging of NATO-wide science & technology resources, facilitator for industry-private sector and military dialogue and operational experimentation, provider of limited funding for R&D and acquisition.

Outlying ideas

NATO should look at which EDTs may or will be dominated by non-Western nations to drive efforts to counter, compensate, mitigate, or prevent.

NATO should consider what NATO can or should provide / contribute to Indo-Pacific partner priorities in defence and security.

Recommended policy and the way forward

NATO should:

Develop and share a high-level "grand strategy" to drive innovation and EDT adoption. The strategy should be comprehensive from creating the conditions for a dynamic, responsive innovation ecosystem through the development process (identification, test, learn, refine, iterate, validate, scale) to delivery, adoption, and integration. This grand strategy should include the purpose of innovation and EDT adoption, the roles of NATO stakeholders and external players, and the ways and means to ensure dynamic, accelerated, and effective (interoperable, high impact) innovation and EDT adoption. An external and frank audit of how NATO currently facilitates innovation and EDT adoption with respect to NATO ambition may help identify key areas for improvement.

Adopt a systems approach to EDT capability integration (e.g., DOTMLPFI – doctrine, organization, training, material, leader development, personnel, facilities, interoperability), and life cycle management and sustainment, including in-life modernisation and obsolescence management.

Improve the quality, depth, and breadth of dialogue with private sector players to leverage the full spectrum of private sector contributions to NATO innovation and EDT adoption. Communicate defence needs as discrete (but sufficiently broad) concepts of operation that would enable and leverage the private sector's ability to creatively develop innovative approaches. Continue to improve and broaden dialogue with private sector to better leverage the spectrum, variety, and breadth of expertise that industry, academia, and civil society offer. The NATO Industry Advisory Group should continue to broaden its inclusion of the full breadth of the commercial sector (from large industries to SMEs to startups and non-traditional defence industries). Map out the NATO innovation ecosystem (including NATO Headquarters, NATO Military

Authorities, S&T Organisation, Agencies, etc. across the NATO enterprise, not just DIANA and the NATO Innovation Fund) for external actors and internal stakeholders.

Focus innovation on those EDTs (or new applications of existing technologies) that add greatest value for NATO's priority defence challenges, especially those that need military input and guidance and funding to respond to priority defence challenges. Adopt now those EDT with immediate military application (e.g., dual-use COTS) and, if necessary, test, refine, validate, scale, and integrate (DOTMLPFI approach).

Follow through with full resourcing and refinement of NATO innovation initiatives (i.e., DIANA, NATO Innovation Fund) and accelerate and expand as possible to exploit their potential.

Adopt agile development and acquisition principles to accelerate development and delivery and improve opportunities to better leverage contributions from private sector to address defence problems. Promote modularity, compatible digital backbones, and NATO standards. *Revise NATO resource and capability development processes* to improve agility, enable rapid iteration, allow for failure, and accelerate development and delivery.

Use market incentives and levers to promote defence-related research, development, testing (e.g., meritocratic competitions) and experimentation. Leverage all domain opportunities for operational experimentation. NATO stakeholders are already collaborating in the maritime domain – NATO's Maritime Command, NATO S&T Organisation, Centre for Maritime Research and Experimentation, and Allied Command Transformation. This is not yet the case for NATO Air Command, Land Command or other operational forces.

Improve adaptive, responsive military concept development to accelerate and improve adoption of maturing EDT (i.e., concepts of employment, doctrine, and TTPs).

Account for data and cyber security, supply chain security, climate change-related requirements (and others) in the NATO innovation and EDT adoption processes.

Enable scaling through aggregation of demand in terms of common requirements and defence investment related to innovation and EDT adoption. This is already a focus of NATO's Defence Production Action Plan, but it needs expanding beyond munitions procurement.

Address technological literacy among policy makers, decision makers, resource managers, and operators. Consider adaptive adult learning, scenario-based experiences, and simulations to provide high-impact training and education to leaders with limited time.

Clarify and define interoperability requirements early during innovation and EDT adoption. This requires policy focus to identify at what level and where interoperability standards are needed and what doctrine or concepts may be needed first. NATO Digital Transformation will advance interoperability in data, connectivity, and networks and should be implemented rapidly as a foundational enabler for EDT adoption. Likewise, NATO's Multi Domain Operations Concept and Implementation Strategy will be drivers for interoperability requirements (see Warfighting Development Imperatives). Despite the overall principle of interoperability, some variety and diversity are desirable as they can complicate adversary response and create tactical (and operational or strategic) dilemmas. NATO should allow for groups of allies to set norms and standards for exquisite capabilities that are unique to a limited number of nations (e.g., offensive cyber, space-related capabilities, hypersonic systems).

Working Group 2: Military Strategy and Future Force

Chair: LTG (Ret.) Ben Hodges (US)

Former Commander, US Army Europe (TAG)

Co-Chair/Rapporteur: Diego Ruiz Palmer (US)

Former Special Adviser for Net Assessment, Defence Policy and Planning Division, NATO HQ

The Military Strategy and Future Force Working Group offered a vision of a revised Alliance Military Strategy and an Allied future force in 2035. Specifically, the working group sought to better understand 1) what changes and new factors (China? Climate? Resurgent Russia? Iran? Advanced technologies?) should be addressed in Alliance Military Strategy (approved in 2019) to prepare for the foreseeable threats and challenges of 2035, and 2) how should such a future force be conceived, generated and fielded in order to be maximally capable of deterring and defending against threats, responding to challenges, preventing crises, and securing nations against hybrid activities? What specific lessons can be drawn from current wars (e.g., Ukraine, Nagorno-Karabakh, Libya...)? How are multi-domain operations changing and how will they change the character of warfare? What implications do multi-domain operations concepts have for military strategy and future force concepts and structure? What new organisations and concepts will be needed for manoeuvre, fires, air and missile defence, mobility, and counter-mobility? What new organisations and concepts will be needed for C4ISR, including electronic and cyber warfare? What new organisations and concepts will be needed for sustainment, maintenance, and military health and casualty care? What critical interactions will be needed with civilian partners (government, industry, academia, civil society) to enable a whole-of-society approach? To enable resilience and defence against hybrid activities (including information warfare)? How should civil-military cooperation and resilience be address in a revised Alliance Military Strategy?

Angus Topshee (Canada), Commander, Royal Canadian Navy

Fin Monahan (UK), Director, Development, Concepts and Doctrine Centre, Ministry of Defence

Karl-Heinz Kamp (Germany), former Ministry of Defence (TAG)

Patricia Lewis (UK), Research Director, Conflict, Science & Transformation, Chatham House

Stuart Peach (UK), former Chief of Defence Staff and Chairman, NATO Military Committee (TAG)

Will Strickland (UK), Assistant Head Concepts, Futures Directorate, Army Headquarters

THE REPORT

1. Background

The WG started its consideration of its mandated topic from the baseline of NATO's 2019 Military Strategy (the first such strategy since the 1967 MC 14/3 *Flexible Response* strategy) and the 2022 New Force Model, which together set out the Alliance's assurance, deterrence and defence missions in the post-2014 security environment and the revised Allied force structure required to execute, if necessary, NATO's new family of advance plans. This baseline provided the backdrop to addressing what kind of challenges and requirements a revised Military Strategy and adapted Force Structure would need to address in 2035, although there was no attempt in the WG to try to draft even the outline of such a Strategy or the main features of future forces.

2. Core Message

While acknowledging the challenge of imagining what NATO's security environment might look like in 2035, the WG agreed the following **Core Message**:

The Alliance must prepare and adapt for a security environment and a combination of threats that will likely be much more complex, complicated and challenging than those existing at the present time. These threats will be multi-directional and multi-domain, spanning the continuum of conflict and the spectrum of emerging technologies. Vectors of threat will worsen on all of the Alliance's flanks: the Eastern Flank, from Russia; the Northern Flank/Arctic, predominantly from Russia, but also, increasingly, from China; the Western Flank (along the Western seaboard of North America, which is NATO's Western boundary) from Russia, China and North Korea; and the Southern Flank, from Iran and terrorist groups, but also growing regional instability and uncontrolled migration flows in and from Africa and the Near and Middle East. Russia is no longer just an Eastern Flank threat to NATO, it is increasingly a 360 degree threat, because of its belligerent posture in the Arctic, the Mediterranean and Africa.

Confronting this much more adverse environment will require NATO to continue to adapt its military strategy and forces, notably by acknowledging explicitly in its Military Strategy the transformational impact of new technologies on future warfare and their potential to make NATO stronger. Applications with the greatest potential to enhance NATO's deterrence and defence posture positively, along the competition-crisis-conflict continuum, include:

(i) collective situational awareness;

(ii) common threat recognition;

(iii) agile decision-making; and

(iv) tailored responsiveness.

Achieving this outcome by 2035 calls for NATO to adopt an "end-to-end" approach to technology management that emphasizes urgency, priority and speed of delivery. Implementing such an approach to technology will require, in turn, greater political engagement and resource investment, as well as institutional and procedural reform. Pursuing such an "end-to-end" approach institutionally and procedurally would require, for example, rethinking the linkages and sequencing between Allied Command Transformation's *NATO War-Fighting Capstone Concept* (NWCC), the NATO Science and Technology Organisation's *Science and Technology Strategy*, the NATO Defence Planning Process (NDPP) and the development of NATO Standardisation Agreements (STANAGs). Two areas of greatest need and potential for implementing such an "end-to-end" approach to technology management were identified as:

(a) Command and Control (C2); and

(b) Integrated Air and Missile Defence (IAMD),

not the least because both are areas of recognised NATO operational competence.

3. Main themes

Main themes discussed in relation to the enabling role of new technologies included:

- In support of deterrence, defence and deception, including the posing of operational and strategic dilemmas to adversaries; the operational endurance of forces; and the simplification of institutional complexity in an organisation such as NATO, through a combination of complex systems' theory and artificial intelligence;
- In achieving positive effects of scale, rather than mass, to undermine and overwhelm the adversary;
- Their positive impact on the trade-off between technology and manpower, taking into account future personnel recruitment and retention challenges, as well as on energy use by the military, in support of system propulsion, system operation and overall operational capacity; and

- Their potential to revolutionise war-gaming, experimentation and technology demonstration. In this area, reference was made to giving current NATO efforts greater weight and salience, in the areas of ISR (*Unified Vision* experiment), electronic warfare (MACE/EMBOW trials), and combined operational capacity (*Combined Warrior Interoperability Experiment*).
- Their applicability to education and training of military and civil audiences to achieve and maintain higher levels of professional competence and help proliferate comprehensive approaches to crisis management and the conduct of war, including the development of agile strategic communications (STRATCOM) capabilities.

4. Obstacles to delivery

There was a clear recognition that in an alliance as large as NATO, composed of a relatively small number of large and militarily capable Allies and many smaller, less capable Allies, the collective quest for effectiveness and efficiency, notably through strengthened cooperation, burden-sharing, pooling, and economies of scale, would assume greater importance. **Key obstacles** on this path would include:

- Institutional fragmentation within NATO;
- A lack of sufficient delegated authorities from Allies to designated NATO bodies;
- A general unwillingness of nations to cede sovereignty to international bodies, in relation to discretionary managerial authority; discretionary budgetary authority; initiative; and disposition of assets;
- Competing operational requirements among Allies and between NATO and Allies;
- Uncertainty regarding the desirable scope of substitution of humans by machines; and
- The absence in democracies of a “war economy” policy framework that would facilitate innovation and authorise risk-taking (although President Macron mentioned the need to transition to a war economy in June 2022, in part in recognition of French operational endurance shortfalls).

5. Findings

There was a general view that the urgency of leveraging and applying new technologies in support of strengthened NATO deterrence and defence, including in the direction of a multi-national Multi-Domain Operations (MDO) capacity, mandated employing pre-existing structures and processes, while pursuing institutional and procedural adaptation in parallel.

As identified under Section 2 above, there were plenty of areas of interest and structures and procedures already in place that could be better exploited to accelerate technological change, particularly in support of fit-for-purpose NATO C2 and strengthened NATO IAMD. To achieve these ends, Allies should be prepared politically to encourage much greater collaboration between various NATO bodies (NATO Headquarters, the NATO Command Structure (NCS), NATO agencies, Centres of Excellence, etc. to create virtuous “clusters of excellence”).

In the C2 area, there should be much greater, politically-mandated engagement between the NCS and the NATO Communications and Information Agency (NCIA) to ensure the early introduction into service of a 21st century digital C2 backbone, whereas in the IAMD area, there should be much closer engagement between the NATO IAMD Committee at NATO Headquarters, SHAPE in Mons, HQ AIRCOM at Ramstein air base for the air force dimension of IAMD, HQ LANDCOM in Izmir for the surface-based dimension of IAMD, HQ STRIKFORNATO in Lisbon for the maritime aspects of IAMD, the applicable Centres of Excellence in France, Germany and Greece, and nations.

There was a general view that a combination of advanced information and communications technologies, AI and quantum computing could significantly contribute to rapid progress in the C2 and IAMD areas and show the way in other areas, building confidence among the Allies on the benefits of new technologies and NATO's institutional and operational capacity to leverage them to the benefit of all.

In addition to NATO's unique institutional role, there was a view that Allies should also better leverage NATO's Framework Nation Concept (FNC), as the UK did through the Joint Expeditionary Force (JEF), to pool and share national and multinational efforts under the helpful lead of willing and able framework nations.

A future NATO Military Strategy would need to show the way on how technology could help overcome gaps in operational capacity among Allies and achieve, through a migration strategy, discrete, higher levels of combined operational capacity. Only a top-down, politically-mandated approach could help create the momentum necessary within the Alliance to overcome national and institutional barriers on the way to such a multinational MDO capacity.

6. Outlying ideas

The implications of the kind of technological transformation discussed in the WG and reported above for the future shape of Allied forces were addressed only at the margins. For instance:

- What could be the impact of seeking technological superiority on the traditional force structures that have been in place since World War Two: Air Force squadrons; Army brigades and Navy task groups?
- Are those force structures inherited from the 20th century viable in an operational environment increasingly dominated by new technologies?
- If they are, what adaptations, including new operational concepts and tactics, would be necessary to keep them fit-for-purpose?
- And if they are not, what alternative force structures for 2035 are imaginable and desirable?

There was also a conversation on the periphery of the main discussions on the management in democracies of the debate between the attractiveness of technological transformation and entrenched institutional and political risk aversion.

7. Recommendations and way ahead

Recommendations clustered around four key ideas:

(i) Spread across the Alliance a sense of urgency in relation to the risks of not leveraging sufficiently, and on an organised basis, the benefits of new technologies for strengthening the combined operational capacity and political unity of the Allies;

(ii) This greater sense of urgency should lead to adopting an "end-to-end" approach to technological innovation and transformation among the Allies and across the Alliance; this comprehensive approach should incorporate political, institutional, procedural, operational and industrial dimensions, possibly starting at the forthcoming 75th NATO anniversary summit in Washington, D.C., in July 2024;

(iii) This deliberate and comprehensive approach to technology should be driven by the concept of "participatory enterprise", where national governments, international organisations and industry, including technological start ups, enter into a compact to structure and accelerate the transformation of defence and security; and

(iv) Be prepared to address with civil society the potential risks and constraints associated with increased technological dependencies, from the standpoint of national security policy, civil-military relations and ethics.

As this report hopefully makes clear, while the forthcoming technological revolution brings along military risks as well as opportunities for the Allies, it also requires a broader, more holistic, more imaginative and more innovative approach to defence policy-making and defence organisation. This means that alongside the forthcoming technological revolution, defence establishments and the armed forces must initiate and manage competently a conceptual revolution of possibly unprecedented complexity and consequence.

Working Group 3: Capabilities Working Group

Chair: Robert Bell (US)

Chief Executive Officer, National Security Council LLC (TAG)

Co-Chair/Rapporteur: BG (Ret.) Robbie Boyd (UK), Gartner (TAG)

The Capabilities Working Group considered how foreseeable threats and challenges of 2035, emerging and disruptive technologies (AI, autonomous systems, big data and ICT, energy and propulsion technologies, hypersonic systems, electronic and electromagnetic technologies, space-based capabilities, quantum technologies, novel materials and advanced manufacturing, and biotechnology human enhancement), and future operational concepts (i.e. Multi-Domain Operations) will affect future capability requirements and capability development. What domain-specific (land, air, maritime, cyber, space, and cognitive domain) and multi-domain (e.g., C4ISR, IAMD, long range strike...) capabilities will be most critical for future deterrence and defence, crisis prevention and response, and resilience? What capabilities will be most affordable, most effective, most difficult to achieve? What capability development strategies and approaches will be most important and / or effective in achieving critical defence capabilities, including those capabilities needed for national and Alliance resilience? How can nations and the Alliance best resource critical defence capabilities to ensure adequate defence investment in research and development, fielding, readiness, and sustainment? What challenges must be addressed in future capability development (e.g., interoperability, supply chains, digitization, energy efficiency...) and how best to do so? What dual-use capabilities will be most important for deterrence and defence and / or resilience? What synergies might be possible between defence, security, and domestic needs? What future capabilities might improve affordability of national, Alliance defence?

Becca Wasser (US), Senior Fellow, Defense Program, CNAS

Bruno Tertrais (France), Deputy Director, Fondation de la Recherche Strategique

Chris Harper (UK), Managing Director, CH4C Global (TAG)

Meia Nouwens (Netherlands), Senior Fellow for Chinese Security and Defence Policy, International Institute for Strategic Studies

Khurram Jamil (Denmark), President, Global Markets, Area 9 Lyceum

THE REPORT

Principal Recommendations

1. The strategic environment we will face in 2035 will be bleak. Russia will remain a clear and present danger regardless of the outcomes in Ukraine, distinguished by the possibility of high intensity, industrial-scale, high-end warfare in central Europe. This will be compounded by an expanded long-term threat from China. Additionally, there will likely be enduring challenges from N Korea and Iran. State threats will dominate but the realities of terror driven warfare will not disappear.
2. Taken together, the nature of the 2035 threat will likely be high-tech, industrialized, protracted, and will require whole of government, fully mobilized, resilient, national responses, including incentivizing industry for surge capacity and protracted production. The budgets generated to finance these must be affordable. But, they will require further increases – there is no peace dividend now in sight.
3. No one nation will be able to respond adequately to address this wide spectrum of threats alone. Responses will need to be founded on cooperation and integration of allied and like-minded partner nations, both in the NATO and Indo-Pacific regions (emerging examples will include AUKUS and other regional groupings such as the UK Joint Expeditionary Force (JEF)). This will require cultural change, including more technology transfer, interoperability, standardization, joint procurement, logistics and sustainment.

4. The biggest risk we face is time. We will lose our already tenuous competitive advantage against our threats if we fail to make the necessary bold adaptations, which include optimizing political and military cooperation frameworks to integrate new EDTs at pace in multi-domain concepts at scale (for example; the Replicator and DIANA initiatives and the NIF and emerging JEF capabilities funding mechanisms).
5. We have an advantage: our recognition that this is a moment not experienced for some time, which if seized can put us in a position to field capabilities in 2035 that will remain functional until 2060 in some cases. Our advantage, then, is the collective 'Western' unity of purpose against the distinct put increasingly aligned State threats we face.
6. This provides the opportunity for accelerated adaption and learning through pragmatic change management, which in turn requires vision and top-down leadership empowered by clear guidance from statesmen.
7. This also means our capability strategies and approaches must be adapted and accelerated, our adoption of tech and integration processes has to be focused on generating speed, while ensuring effective testing, experimentation and demonstration. This will require closer partnerships with industry to adapt and adopt new acquisition and sourcing processes. Nonetheless, we must also maintain the established processes that work and sustain our legacy systems while seeking out new methodologies (with industry advice) to do this. The NATO Defense Planning Process (NDPP) plays a necessary role. But, it must be complemented by vanguard groupings under lead nations that can and will go faster if provided with innovative investment funding mechanisms.
8. *What does this mean for capabilities?* We think that the emerging and disruptive technologies such as AI, Quantum, Big Data, improved processes in digital sourcing et al, will need to complement and improve legacy capabilities but also they will enable the following key capability categories:
    a. **Manpower.** This is the most precious capability we have. We will need to build beyond our standing forces – new ways of generating threat-focused reserves, improved civilian engagement and in some cases possibly reintroducing conscription. The looming demographic trends are ominous, so we will need tech to replace the human where safe to do so as well as the education our societies on the threats to encourage all to play their part.
    b. **Nuclear weapons will endure.** The era of strategic arms control and unilateral reductions is over. There will need to be significant re-education of society and increase in resilience. New technology and decisions on missile defences will follow. Organizations like NATO may be suited to integrate and orchestrate more strategic enablers.
    c. **Autonomous Systems** in all domains including responses such as Counter-autonomous systems in all domains will increase. This will require values and international legal examination. Perhaps additional rules of war.
    d. **Legacy systems** will endure but must be repurposed and consistent with adapted warfighting doctrines.
    e. **Survivable C2** with secure communications will become more important, enabled by a globally interoperable Secure Cloud system. Mission command philosophy will endure and becomes more important with built in requirements for dispersal and other survivability methodologies emerging as critical capability drivers. There will be a step change linked to Multi-Domain Operations requiring secure linkages and a willingness of national civilian and military elements to subordinate themselves to lead nation 'vanguard' groupings.

f. **Sustainable energy and materials.** Supply chain management will be more affected at source for critical rare earth materials and fuels. Stocks of material will need to grow to ensure industry can respond to surge **production activity.**

Background, Context, and Discussion

'*[It is all about] *Capabilities, Capabilities, Capabilities'.

Lord Robertson when the NATO Secretary General

Under the Chair of Dr Robert Bell and Co-Chair Brigadier (Retd.) Robbie Boyd, a Working Group (WG) to examine the capability outcomes for future war and deterrence. Our most important and relevant observations out to 2035 are summarized above. Our methodology and assumptions - summarized below - concentrated on three factors where new technology consequences will have an impact; firstly, a collective agreement on the 2035 threat environment. Secondly, where the opportunities existed to refine and exploit Emerging Disruptive Technologies (EDTs) and thirdly, to seek opportunities to harness new operational concepts to refine and promote our deterrence posture. Whilst seeking opportunities, the WG also noted there was a need to reconcile opportunities against three further criteria – affordability, orchestrating new tech with legacy tech, and generally ensuring national and collective resilience improvement.

In the context of affordability, the WG considered how best the dimensions of affordability and resilience can reinforce deterrence credibility, given competing demands for national public finances. At a macro level, the WG noted with concern the recent Canadian Prime Minister's admission that Canada was simply not going to reach NATO's 2% Defense Investment Pledge (DIP) despite having been embraced by Canada at the Wales Summit and reaffirmed at the Madrid Summit. The WG emphasizes the importance of the 2% goal and regards it as a "floor" for each ally's investment. The WG also emphasizes the importance of the accompanying commitment to dedicate at least 20% of national defence spending to R&D and procurement and views this level of investment as essential to achieving NATO's EDT and capabilities objectives. [The 2% and 20% metrics of the Wales DIP 2014 are the two so-called "input" metrics. It also includes the commitment to focus that spending on nine so-called 'output' metrics that provide guidance on how best to ensure that the spending is made smartly and in line with NATO's agreed capability requirements, as allocated pursuant to the NDPP in line with agreed threat assessments.[1]] We noted positively that due to sober reflection regarding Russia's aggression from 2014 and since February 2022, and the emergence of China as a global threat and Iran and North Korea as regional threats, there has been progress amongst allies towards meeting the 2% minimum threshold. We noted that recent events in Gaza and elsewhere would mean terrorism would also remain a threat in 2035 and would still need technological exploitation of EDTs to deter it.

1. 1Percentage of air, land, and naval forces that are deployable;
2. Percentage of deployable air, land, and naval forces that can be sustained in deployment;
3. Percentage of deployable air, land and naval forces deployed on NATO Operations and Missions abroad;
4. Percentage of deployable air, land, and naval forces deployed on non-NATO Operations and Missions abroad;
5. Percentage of deployable air, land, and naval forces deployed on in support of NATO Assurance Missions;
6. Percentage of Capability Targets allocated to that ally in accordance with the NATO Defense Planning Process (NDPP) that have been met;
7. Percentage of billets within the NATO Command Structure assigned to that ally that have been filled;
8. Percentage of billets within the NATO Force Structure Headquarters assigned to that ally that have been filled; and
9. Contribution by that ally to the Immediate Response Force (IRF) of the NATO Response Force (NRF).

Fair burden sharing underpins affordability. Not one nation could field a full spectrum of capability, even the USA would be challenged between multiple NATO area, China and regional state threats. The NATO guidance that one nation should not be expected to provide more than 50% of any one capability led to reflection that international groupings and lead nation groupings could accelerate capability fielding and interoperability. It was also considered that larger international groupings, such as NATO, were particularly suited to generating strategic enablement capabilities – for example Missile Defence systems. We noted that in Europe there was probably an underestimation of the Chinese threat in every domain.

Affordability will require more cooperation. This was most manifested in the sharing of tech amongst allies as well as securing supply chains (and in some cases stockpiling material). Supply chains were at their most vulnerable at the point of origin, with many rare earth materials gradually moving to Chinese control across several continents and in the case of French nuclear fuel challenged by Russia in Africa using Wagner Group-type activity to destabilize. There was a need to engage as one and incentivize nations to sell commodities. Our general publics still do not understand our State security risks and are less inclined to spend state funds on it. An innovative suggestion included encouraging pension funds to invest in Defence innovation and capabilities to amplify the public covenant towards defence spending.

Finally, our WG discussion reflected on the more micro affordability issues. Individual education and training, platform procurement and tactical ways in which deterrent effect could be generated. Often new ways were less expensive than old lethal alternatives. This was people-based, enhancing the WG conclusion that manpower was our greatest capability but it needed to be guided and nurtured.

The WG considered where EDTs fitted into capabilities and acknowledged that existing processes that generated targets based on deterrent plans (for example NATO's NDPP activity) were still relevant for the acquisition and sustainability of legacy systems. A mix would be required, technology enhanced legacy capabilities as well as new EDT ways to deliver our deterrence ends. EDTs were more often than not a silver bullet. Careful integration and orchestration with legacy capabilities would drive effect. This would require a change in C2 methodologies and in particular the sourcing of tech and digital solutions with industry to maintain speed of relevance in fielding capability. Our existing sourcing processes were too slow. We recognized that it took time to field some capabilities and welcomed new investment in innovation companies through initiatives like NATO DIANA, NIF and fresh capability funding ideas like the 'JEF Bank' to generate speed through smaller grouping of vanguard nations. Above all else we considered that time was our biggest risk.

The WG also highlighted the challenges to greater industry cooperation. Identifying new innovation through start ups, then protecting their development from absorption and exploitation by Prime Companies threw up IP ownership issues. Technology often needed to be dual use (civilian and military) to make it commercially viable. But also, the case of Space X raises questions as to how far an innovative capability company should be allowed to go before it is eventually nationalized? The recent example of Elon Musk entering in to operational level decision-making over Ukraine support was notable.

Quantum technology raised concerns for both C2 systems and also for submarine based nuclear deterrence, though the WG was of the view that no breakthrough that would "make the oceans transparent" is imminent. A discussion ensured on diversifying systems where ultimate deterrence would continue to come from legacy nuclear systems. But C2 had to be protected. A spiral of action and reaction of Quantum response was envisaged, making this technology particularly vulnerable to a [Dreadnought style] tech arms races.

Resilience discussions highlighted that alternative demands for precious resources would require risk-based prioritization of which tech to back and where to concentrate on (re)building national resilience. Lessons from Ukraine (particularly on holdings of stocks of ammunition) raised higher priorities for (re)investment that perhaps technology. It was noted that we are unable to fully predict our logistic demand to fight a major war in Europe and the group pondered the prioritization of resources. Industrial scale warfare was expensive but back. Could industry ramp up production in time if our stocks failed to buy enough time?

Climate change impact was considered. There would be opportunities from emerging fuel technologies, which in resilience terms would drive the need for more energy self-sufficiency as a prioritization for many governments. There was also a significant issue with manpower reliance – demographics in the 'West' were not encouraging and where rearmament, logistics resilience and improved C2 systems were driving significant increases in the DIP (for example in Poland) it was perhaps inconceivable to see how manning such force increases could be done without significant societal changes in education, training and ultimate reserve generation. Conscription in some Western nations was becoming a more likely option. The WG reflected how that could be achieved given current population expectations. Autonomous systems were one way to help with manpower shortages but were only emerging with recent advances in AI.

Working Group 4: Industrial Implications and Procurement

Chair: **Professor Holger Mey (Germany),** Vice President, Advanced Concepts, Airbus Defence and Space (TAG)

Co-Chair/Rapporteur: **Joe Robinson (UK)**, CEO, Skyral Group

The Industrial Implications and Procurement Working Group focussed on how best to achieve and accelerate the development and fielding for future capabilities based on emerging and disruptive technologies. What innovation ecosystem (e.g., public / private / industry / academia / military partnerships, public/private funding, structures and processes) is needed to meet the future war challenge (deterrence and defence, crisis prevention and response, resilience) and how can that ecosystem be created? What are the most important obstacles and challenges to address to achieve and accelerate the development and fielding of future capabilities, including national and collective capabilities? How can nations and the Alliance incorporate best practices and enabling technologies (e.g., AI, digital twins, extended reality tools, modelling and simulations, new materials and advanced manufacturing, public/private cooperation) to accelerate research and development, testing and experimentation, and rapid scaling to meet security and defence needs? How can these best practices and enabling technologies reduce risk, reduce cost, reduce climate impact, and improve life cycle management (e.g., sustainment, supply chain security, upgrade, replacement and recycling)? What kinds of defence capabilities are best provided as a service while ensuring security of supply, effectiveness, and responsiveness to contingency and increased demand? What considerations and factors still need to be addressed in NATO and EU policies, structures, and funding mechanisms (e.g. DIANA, NATO Innovation Fund, European Defence Fund, PESCO, NATO / EU armaments cooperation) to best provide future critical capabilities?

Barbara McQuiston (US), Chair to the DIANA Board of Directors, Department of Defense

Giampaolo di Paola (Italy), President, AEREA (TAG)

Kevin Billings (UK), Hon Group Captain, Anduril

Martin Cronin (UK), Chief Executive, Syniad(

Roelof Van Der Spuy (UK, South Africa), Strategic Advisor at Teledyne

Trygve Refvem (Norway), Executive Vice President (Ret.), Norsk Hydro (TAG)

THE REPORT

Question: *How best to **achieve** and **accelerate** the development and fielding of future capabilities based on emerging and disruptive technologies.*

Core message

Effective adoption of new technology will provide a strategic advantage over our enemies which can improve both deterrence and the chance of victory in combat. This edge is best defined today by 2x overarching functions: 1) Increased speed of understand-decide-act cycle, leading to improved tempo of operations and 2) Increased lethality through increasingly smart autonomous systems. Both of these functions are, ultimately, the result of innovations in software. However, this is all for nought, without effective adoption: bringing new technology to bear on the mission. Governments have an innovation adoption problem, not an innovation problem per se. If we are to be serious about fixing this challenge, leadership at the highest level must focus on fixing this adoption process and be accountable for pulling through new technologies: from research to production capabilities. It is not enough that our leaders are seeking to understand new technologies - that is only the first step - they must assign time

and effort and make it their business to reform the policies that add friction to innovation pull through, shorten the processes, better align incentives and create a culture that embraces risk in a different way. There are fantastic examples of innovation adoption models in the alliance, we should be thinking of Picasso: Good artists borrow, great artists steal. Nations should steal these great examples, don't reinvent the wheel! Private sector will continue to be the beating heart of innovation (70% of all R&D comes out of the private sector) due to economics and talent. Commercial innovation will continue to accelerate as AI increases the productivity of industries. The effective adoption of dual use technologies will increasingly become essential to delivery of cutting edge capabilities.

Main findings:

There were 4x main findings that we believe can help **achieve** and **accelerate** the fielding of future capabilities based on emerging technology: 1) Fix adoption, 2) Focus on partnerships, 3) Embrace new business models and 4) Government as an investor not just a customer.

1. **Focus on fixing the adoption of new technologies not on the tech itself.** There needs to be an urgent focus on reforming the process and policy to fix innovation adoption. It's not about the tech, it's about reforming the process to adopt the right tech. Leaders in senior roles must make this one of their priorities here. There are few things that very senior leaders can focus on - we believe this innovation adoption is so important to deterrence and victory, that a senior leader should own this reform and make a stand to make it one of their very few missions. Without this focus and publicly declared accountability, effective innovation adoption will not happen at scale.
    a. **Work back from the outcome.** Useful, practical and appropriate technology matters. This comes from focussing on rapidly testing, trialling and fielding new technologies that generate effects and, ultimately, new capabilities. Need to focus on delivering mission outcomes and work back from that.
    b. **Incentives are an issue.** There needs to be a clear and transparent alignment of incentives, where every stakeholder involved in procurement and program delivery is incentivised to achieve outcomes and **are not** incentivised to simply follow existing processes successfully.
    c. **Measure success against new technology fielding**. Metrics like SOCOM's process - 590 days 185 days; 3 documents 1 document, 17 stages of review 9 stages of review - to keep us honest about how well we are doing and incentive program managers to remove friction and blockers.
    d. **Government is a fantastic early adopter.** History has consistently shown this. There is an opportunity for the government to market themselves as the gateway to sell new tech into commercial space in order to attract dual use technology companies to the sector.
    e. **2x motions to effective adoption: Brown Field and Green Field.** This is both about integrating software into existing hardware (brown field) and pulling through new capabilities (green field). Both have different challenges.
        i. **Brown field**: Effective Integration between current capabilities and new technologies matters. Modern software needs to be integrated into existing (procured or budgeted) hardware to ensure that near term platforms are able to be upgraded rapidly and empowered with the latest technology (ML, data processing and dissemination, AI, computer vision, data fusion etc).

ii. **Green field:** This is about leaping the valley of death between pilot and production capabilities. We must Learn from where this process and policy reform has worked: UORs, Ukraine procurement, DARPA, SOCOM, DIANA. There are great examples in the ecosystem. They need to be understood, stolen and scaled. We should be aiming to achieve less than 3 months from successful pilot to production cap to keep SMEs alive). A proposed process to do this would be: see 1) Issue a challenge/problem to the market (get as many ideas as possible), down select (via demo, paper and interview - speed matters here), get mentors in place to support the downselected companies. 2) Test, demo and experiment on the mission and downselect successful test examples 3) deploy production capability linked to programmatic acquisition budget. Ensure the accountable nation is prepared for catastrophic success. A good model of this is the Transition Confidence Level (TCL) from SOCOM, which covers policy, procurement and enabling conditions: e.g.) data, processing, networks amongst commercial reform.

2. **Partnerships:** Innovation adoption needs the right partnership behaviours to be successful:

    a. **Role of Government as a good customer for Industry**: IP rules need to be more favourable. There needs to be more regular and rapid competitions. Software centric contracts need to be shorter, more flexible and performance based. There is no need for “bad lock-in” with software platforms and software centric hardware that are built on open standards. There is an opportunity for good lock-in through ecosystem value and benefit of the speed of integrating new best in class technologies. At each phase of procurement, companies must be able to make a profit. The delivery of new, relatively risky capability involving new tech, is hampered when desired outcomes are not communicated to industry in a timely and regular fashion - especially as they evolve. Stretch goals should be put into programs, with a big contract at the end of it, to encourage more risk taking and innovation in industry. There is a need to update the export of critical technologies criteria for ITAR and other national export requirements. Export policies are restrictive (especially US), they need to be revised in the age of software centric systems as this affects industrial strategy, especially decisions around where global companies develop their products. ITAR should move from an “assume ITAR and find a reason not to apply it” to “assume no ITAR and find a reason to apply it”. There are unintended consequences of ITAR (and similar national strategies) which encourages wasteful practices across the Alliance. Risk needs to be viewed through the lens of speed and time as the key variables. Fielding new technologies slowly to minimize risk is not only an incorrect interpretation of risk, it is damaging our ability to retain the edge. The need for faster fielding is a result of the threat and a function of pace of technological change.

    b. **Role of bigger industry supporting small industry:** Mentorship and support from those who have served with successful Primes or tech companies that have scaled in Gov market is critical to support long term growth of SMEs. This needs to be done without risk of IP or talent theft.

c. **National Industrial policy needs to be carefully balanced with capability needs**: Defence industry is a national asset - sovereign support for the defence industrial base is alive and well, especially in Europe. We need to accept that the defense market is not necessarily a free market. But when any procurement is done, the authority needs to communicate the weighted scoring criteria on industrial policy vs. best capability regardless of national economic interest. Talent scarcity continues to weigh the dice on industrial capacity to create new technologies. Digital skills are evolving: Gov sponsored digital talent initiatives need to have the agility to evolve as AI shapes the type of skills required.

3. **Business models are evolving, which presents a significant opportunity for faster and more effective adoption:**

    a. New companies are emerging that are funded differently and will behave differently. Expect more as-a-service models as companies present ready baked products to Defence Depts that have been built with their own capital.

    b. **Software has transformed capability and the delivery of effects:** It has enhanced the speed of delivery and capability improvement. It enables faster upgrades, and easier and cheaper through life support. Delivery as-a-service for software: over the air updates are changing the capability game, this needs to lead procurement and buying changes - more renting and expecting a through life service and less buying and owning.

    c. **Dual Use is only going to get more important and prevalent:** A culture of defaulting to bespoke capabilities needs to be changed to a default of “don’t bespoke” with a focus first on COTs to create economies of scale. This needs to be balanced, however, with capability needs - mission needs - which should inform the need to bespoke first and foremost.

    d. **The “culture of security” in defence needs to be challenged**: speed of delivery, rapid iteration and open standards does not mean a capability is less secure to cyber threats or information leakage. Rapid and effective iteration in contact with the mission has been found to make capabilities more reliable and secure, not less. The era of locking software in a box (on prem) is gradually coming to an end.

    e. **Evolution of defence specific standards should be seen as an opportunity.** Military standards and certification needs to be reformed and carefully considered as the wrong standards are stifling innovation (they are irrelevant in software centric programs on open standards) but too loose certifications can be dangerous.

    f. **Success of new software centric capabilities** need to be measured on 2x fronts: improvements to mission outcomes and reliability and quality of through life, evergreen service.

4. **Funding:**

    a. **There is a gap in funding which is preventing adoption**. This gap exists between TRL 3 to TRL 8/9 - pilot to production stage - which is unhelpfully exasperating the adoption problem. Government needs to fill this gap, especially in Europe, where there is a much smaller and more risk adverse VC community. Government needs to double down in Europe as an investor as well as a customer. NIF, NSSIF, In Q Tel are great models; we should steal and replicate them across the alliance and hire in experienced investors to run these funds to deliver a true public private partnership. This is an opportunity to align incentives between government and industry.

Working Group 5: Strategy and Policy

Chair: Jim Townsend (US), former Deputy Assistant Secretary of Defense for Eurasian Affairs and CNAS (TAG)

Co-Chair/Rapporteur: Dr Robert Grant, Programme Director, Wilton Park

The Strategy and Policy Working Group will discuss how foreseeable threats, challenges, and scenarios of 2035 and the changing character of war (based on defence and security implications of emerging and disruptive technologies) will affect NATO and EU security and defence strategy and policy. What might future NATO and EU membership look like? What changes in NATO and EU roles, responsibilities and instruments of power are conceivable, desirable to achieve the most effective outcomes for integrated deterrence, security and defence, crisis prevention and response, resilience? What areas of NATO and EU cooperation are likely to improve or deteriorate and how best to achieve synergy? What challenges will NATO and EU face in the case of a major U.S. engagement in another theatre, and how best might allies and EU member states prepare for such a scenario? What new roles might NATO partners play in Alliance security and defence? What new security structures are needed for European security and defence and regional stability in Europe's periphery? How NATO and EU plan should, prepare, compete, respond, fight and win? What changes may be needed to NATO's 2022 Strategic Concept and existing NATO defence policies or EU's Strategic Compass and European Security and Defence Policy?

Hanna Shelest (Ukraine), Programme Director, Ukrainian PRISM (TAG)

Heather Venable (US), Associate Professor of Military and Security Studies, Department of Air Power, Air University

Rainer Meyer zum Felde (Germany), Kiel Institute of Security Policy (TAG)

Slawomir Debski (Poland), Director, Polish Institute of International Affairs (PISM) (TAG)

Ilmars Lejins (Latvia), Deputy Director, NATO IMS P&C

Vincenzo Camporini (Italy), Scientific Advisor, Institute of International Affairs (IAI), Rome, Italy

THE REPORT

NATO Adaptation in the next decade: the transition from NATO 2.0 in 1990 to NATO 4.0 in 2035

With the end of the Cold War, NATO was faced with re-inventing itself from a wartime alliance to one that was more political than military and focused on creating a Europe "whole, free and at peace." The Soviet Union was no more, leaving NATO without an obvious threat but with an identity crisis. It had to adapt to peacetime which it did; NATO 2.0 enlarged, militarily became smaller, and focused on going out of area. The hopes of the 1990s faded as an aggressive and revanchist Vladimir Putin set out to reassemble the Soviet empire by invading Georgia n 2008 followed by Ukraine in 2014. At NATO's 2022 Summit in Madrid, NATO had to again adapted itself to a new geopolitical reality and became NATO 3.0, one of rebuilding its force structure in Europe to deter an aggressive Russia and face war already breaking out in Europe. Today, NATO 3.0 is rebuilding territorial defence in Europe.

By 2035, there well could be a NATO 4.0 adaptation, shaped not just by geopolitical change but a revolution in military technology beginning in this decade that changes the very character of warfare. There is also the possibility that instead of a NATO 4.0 driving military technology in 2035, NATO will remain at the outdated version 3.0 because the Allies did not move fast enough to stay on the leading edge of technology. NATO's adversaries may have made a different decision.

NATO in 2035 could see the US still in a leadership role but with reduced engagement in NATO, for political reason or because the US is engaged in another theatre, like the Indo-Pacific. If current defence spending trajectories hold, the European pillar at NATO, including Ukraine, may have the capability and willingness to take on more responsibility and fill gaps left by US forces being used elsewhere. But filling those gaps seamlessly will be critical, as the Russian threat to European stability will likely have increased. By 2035, a seething Russia could be in the middle of rebuilding a more professional and capable military guided by lessons from the war in Ukraine, including incorporating modern military technology. A hostile China will likely be seen by NATO as more of a threat than it does today, continuing unabated its military build-up and harnessing new military technology.

NATO in 2035: Does it adapt to 4.0 or remain mired in 3.0?

Given the geopolitics in the years to come driven by threats from Russia and China, NATO and EU security and defence strategy will have gone through multiple adaptations by 2035. At least one and perhaps two new NATO Strategic Concepts will likely have been drafted by then as well as a new EU Strategic Compass. Changes to NATO and EU policy and the resulting staff reorganizations at NATO HQ will likely take place frequently as NATO adapts to the changing strategic environment. Fast-paced technological breakthroughs will also drive changes to NATO/EU strategy as the institutions struggle to stay on top of technological surprise and adapt to its impact on the character of war.

Most importantly, for the first time in 40 years NATO has developed robust regional defence plans all along the frontier with Russia with specific operational deployment objectives and capability requirements for individual allies; NATO has also enlarged its ready forces to 300,000, both are major undertakings. The implications for NATO itself and for individual Allies from these plans are profound, the implications being that the character of warfare has changed since the end of the Cold War and days of counter-terrorism and “out of area or out of business. As 2035 gets closer, Allies will need to retool themselves for a fight on the continent unlike any they have experienced before due to the changes in warfare. In the run-up to 2035, NATO will need to collect and propagate to Allies lessons learned from the Ukraine war (as well as Gaza/Israel war) and push allies to incorporate them through the defence planning process. Many of these lessons will centre on advances in military technology. The NATO defence planning process may have to be retooled as well to ensure capability goals incorporate advances in tech and motivate allies not to fall back on legacy systems.

Ensuring NATO stays on the leading edge of technological change and can adapt at the speed of relevance will become a top priority and will test the political skills of Alliance leadership to ensure Allies and EU members pay the price to invest in changes in hi-tech warfare and not fall victim to obsolescence and legacy thinking.

By 2035, a NATO version 4.0 should emerge, consolidating adaptations since 2023 and dedicated to mastering the revolution in military technology which will dominate warfare in the coming decades. To master the revolution in warfare in 2035, NATO will need not only to continue promising work already started at NATO to harness hi-tech but to raise the profile of tech in NATO’s culture -- especially the priority in NATO capitals, where adaptations must take place. The following describes how foreseeable threats, challenges, and scenarios of 2035 and the changing character of war (based on defence and security implications of emerging and disruptive technologies) will affect NATO and EU security and defence strategy and policy by 2035.

Changes to NATO/EU strategy and policy resulting from the threat environment and the revolution in military technology.

- **Changes to the Strategic Concept and NATO HQ staff structure**

NATO's defence strategy as laid out in its Strategic Concept will likely be impacted in the years to come as NATO leadership give additional guidance to NATO authorities about adaptation they feel is needed to keep abreast of changes in tech. It should be stressed that NATO today is already focused on the impact of tech advances on the character of warfare. However, in the years to come as the pace of tech accelerates (and is influenced by conflict such as those in Ukraine and Gaza), NATO may have to be more nimble in adjusting to change and more insistent that Allies keep up. To do this, NATO will need to play the leading role in the transatlantic community to make sure Allies are not just keeping up with technological change but are incorporating breakthroughs in new military procurement or in their legacy systems. NATO will have to ensure interoperability is not derailed as some Allies incorporate tech innovations (especially in communications) and some do not. NATO defence planning will be critical in the effort to develop and assign capability goals that move Allies forward on using tech and countering tech advances by adversaries.

To increase the visibility and meet the urgency of helping Allies deal with the revolution in warfare, NATO should consider adding to the Strategic Concept a fourth core task of maintaining NATO and the Allies on the cutting edge of technological change in warfare. The suggestion of adding a fourth core task is not taken lightly; adding a new core task is difficult and tasks are focused on meeting types of threats, not military capabilities. But the potential for breakthrough advances in tech that quickly provide an overwhelming superiority to an adversary is a threat NATO cannot let happen. The potential for swift advances by an adversary in military technology to threaten the Alliance in multifaceted ways puts maintaining superiority in technology into a special category of military capability all its own, alongside conventional and nuclear capability. Tech is no longer just an enabler for the other two warfare areas but should be considered a warfare domain in and of itself. To be dominant and master tech warfare will be an all-encompassing task reaching into every area of NATO, and so needs to have the political visibility and punch of a core task of the Alliance, signalling the importance NATO gives of dominating the tech space.

In the years leading up to 2035, NATO will likely undergo further reorganizations of staff to address various aspects of the tech revolution, including planning and training. Pulling together and making more coherent the various strands of tech work already taking place at NATO will be important, as will be NATO working more closely with the private sector and civil society. Giving the fourth core task its own Assistant Secretary General (ASG) for technology that can provide a single focus of leadership is essential; giving bureaucratic punch to an ASG at NATO HQ also signals to Allies the importance NATO gives to keeping pace with technological change as well as giving weight to the issue in NATO bureaucratic politics.

- **Changes to NATO and EU membership**

NATO and EU membership will also be impacted by technological change. In the 1990s, NATO enlargement was geographically focused on bringing on members who could help create a NATO "whole, free and at peace." NATO and EU membership was also the carrot used to motivate the new European democracies to make sometimes painful changes to how they govern before they could be considered candidates for membership. In the years leading to 2035, NATO and EU enlargement should be approached from a different angle. Are there candidates whose strengths may be new thinking and capability in the tech revolution? For instance, Ukraine is more competent in drone warfare and other aspects of the tech revolution on the battlefield than any Allied nation including the US. That alone should be taken into consideration when looking at Ukraine or other candidates for membership. Additionally, by 2035 launching satellites and building drones will not be the province solely of a few nations; many others will be able to bring such capability to the battlefield, thereby bringing the value to NATO of candidates in 2035 not obvious today. The Partnership for Peace should be retooled to create special categories of Partners who excel in tech, such as those nations in the Indo-Pacific like India, who are not necessarily interested in NATO membership or even political

partnership but in a “business relationship” with NATO where both parties can find value in working together on tech. A closer partnership based on working together on military technology can become the pillar of the NATO relationship with older partners such as Australia, New Zealand, South Korea and Japan. Such Partnership can play defence as well…keeping China out by keeping Indo-Pacific nations close to NATO and the EU.

A retooling of NATO partnerships based not just on geopolitics as in the past but on strategic interests like access to rare earths or technological capability important to NATO could look like three circles of partnerships:

a. Traditional partners who are candidate members (Ukraine, Georgia, Moldova) and those who are not candidates but enhanced partners (Japan, Australia, S. Korea)

b. Partners key to stability in Europe’s periphery (MENA, Caucuses)

c. Partners with whom NATO has strategic interests and could form a business relationship (India, partners in SE Asia, Africa and Latin America).

- **New roles for NATO and the EU in 2035**

A “European pillar” at NATO has always been politically present at NATO, especially after the end of the Cold War as the EU raised its ambition to become a major global power. By 2035, the European role will have (slowly) progressed along this trajectory; a strong European pillar at NATO by 2035 should include Europeans taking defence more seriously, with the core of the European pillar residing within EU but with defence and security representation in NATO. Especially if the US presence/engagement in NATO lessens, it may make sense to enlarge the European pillar at NATO by 2035 to include the UK, Canada and Norway.

As the EU changes, the way NATO engages with it should change. Closer NATO and EU cooperation on handling the tech revolution, including with the private sector, will be essential if the West is to keep pace with change. The tech revolution is driven less by government or by military requirements than by competition in the private sector, which in Europe is anchored in the EU. It will be the US and the EU, not NATO, that will regulate and legislate limitations on tech, setting rules that govern how high tech is used by the military regardless of what adversaries may be doing. The EU must have a better understanding of NATO military requirements and can help disabuse negative views about tech’s impact on warfare shaped more by ignorance and disinformation than on how the military would integrate and use hi-tech. The EU can also be a leader in helping European tech industry add value to military applications of hi-tech. Ignorance in both NATO and the EU about hi tech and the military, as well as each not appreciating the responsibilities the other has in protecting the public, will cause ill will and hostility in both institutions against each other that could cause a deterioration in the effectiveness of both institutions of managing the tech revolution.

In addition to roles that build an offensive tech position for both NATO and the EU, there is a defensive game for both as well. Both institutions will have roles, new for NATO, to ensure tech advances in the West do not bleed over into China or Russia. We can use tech to show us where the West is vulnerable to tech leaks and where the tech areas are located that both adversaries are trying to exploit. Such a role is not new to the EU but it is to NATO, NATO’s role should be to provide military advice to the EU to help them build a regulatory wall to stop poaching by Russia and China without doing harm to the tech industry in the West.

- **Strengthening NATO - EU cooperation by 2035**

Security and defence cooperation between NATO and the EU has grown, initially in fits and starts, each year since the 1998 St. Malo agreement between the UK and France that set the EU ambition to build a military capability. This cooperation was difficult to build because of European and transatlantic politics revolving around differing visions for the EU, particularly in the defence area. Greek-Turkish tensions over Cyprus also limited cooperation. Because of that conflict, Turkey has blocked any form of official cooperation between the EU and NATO. However, they have not vetoed informal staff cooperation. Turkish obstruction of formal NATO-EU cooperation will likely continue even to 2035, given the inability of both sides to find

a solution to the Cyprus conflict. Therefore, closer formal ties between NATO-EU to ensure cooperation on military high tech to meet challenges in 2035 will not be likely.

However, this should not stop both institutions from intensifying informal cooperation on military technology in the years leading to 2035. NATO has tended to work on military tech in parallel, rather than in cooperation with, the EU. However, with the revolution in military technology threatening to quickly overwhelm the character of warfare, both institutions should try to break from past patterns and begin joint, or at least coordinated work on military technology, both to better protect breakthroughs in military technology from leaking to China and Russia and to ensure Allies and EU members are incorporating advances in technology in their defence industries and in their militaries.

To help do this, an informal, senior-level NATO-EU coordinating committee on the revolution in military technology should be formed to focus on the rules and regulations the EU (and the US) may be putting on how tech is used by the military and how this will impact NATO's ability to deter an adversary who is not equally as constrained. At the EU, a "Commissar" responsible for tech and answerable to the EU Commission should take charge of military technological development in the EU, with an emphasis on dual use and coordination and interaction with NATO. The NATO-EU committee could also form a closer working relationship with the private sector and civil society.

NATO can inform allies and EU members on defence technology it thinks needs to be protected from leaking to China and Russia. Similarly, NATO can inform EU regulators about high tech breakthroughs that NATO Allies need to be able to access and so should not be kept from military use. This committee could also act as a clearinghouse, informing both sides of advances being made in tech and facilitating US-European industrial cooperation on tech, including coordinating NATO work on Diana with similar EU work in the European Defence Agency and in the PESCO process.

In some ways these EU and NATO approaches to tech are "apples and oranges" given the different defence and security ambitions of both institutions and the differing roles both institutions see themselves playing when it comes to tech. This coordinating committee has to work through these differences to find ways to keep NATO on the leading edge of tech while not running afoul of EU regulations that try to keep the harmful aspects of the tech revolution from impacting society. Already existing committees could be revamped and better optimised to become a coordinating committee: for example, NATO and EU already have weekly consultation on cyber; this group could be reorganized to address not just cyber but coordination on tech as well.

NATO/EU cooperation on military tech issues was non-existent a decade ago. If coordination can stay on an upward trajectory, 2035 should see a closer and more productive relationship between NATO and the EU, with NATO able to meet its requirements within an EU regulatory framework that also prevents tech leakage to China or Russia. Either EU and NATO will step on each other's toes in the run-up to 2035 or will make progress by working together.

- **NATO challenges backfilling for US forces in Europe if they are deployed to another theatre**

Advances in technology can help NATO Allies deal with the capability gaps they could face in 2035 should the US be engaged elsewhere in another theatre, but only if Allies keep pace with technological change. For example, should the US reduce ISR assets in Europe, or satellite bandwidth, Allies could fill the gap with their own UAV or space capability. But if Allies fall behind the tech race and by 2035 Russia has recapitalized and modernized its forces using lessons learned from the Ukraine war, Allied deterrence could be at risk.

- **What new security structures are needed for European security and defence and regional stability in Europe's periphery?**

The proliferation of security structures developed after the end of World War II has made the creation today of new additional structures no longer considered solutions to problems but sometimes part of the problem. For decades, Europe's periphery, encompassing the Caucuses, the Middle East and North Africa, have been the source of instability causing the movement of peoples towards Europe, especially from the MENA. This movement of peoples has been caused by not just conflict but natural disasters, most recently drastic changes in weather conditions caused by climate change. Mass migration can bring with it terrorism and international criminal conduct, as well as humanity in desperate need for relief and the opportunity for a new life. The political conflict immigration has caused in Europe has helped to feed a new wave of extremism in European politics.

Creating new security structures between now and 2035 will not be a popular nor an appropriate response to restoring regional stability on Europe's periphery. Making better use of existing structures such as the OSCE, the UN, the EU and the AU can be part of the solution, if nations in both Europe and in Africa/Middle East have the political will and resources to address the conflicts causing migration problems at its source. The problem is that by 2035 there likely will not be much change in political will or access to resources to address conflict in the periphery.

Addressing the root cause of these conflicts on the periphery of Europe is not considered a NATO project; NATO can help European Allies deal with the security implications of instability, but even then nations would rather address these issues domestically themselves, or work with the EU.

But in 2035, NATO can help provide Allies and the EU with technological solutions to help them deal with instability on the periphery more efficiently than today. For instance, artificial intelligence can help pinpoint the source and causes for conflict in the future, predict where conflict may break out, or what environmental conditions may cause people to move north and where they may go. Political instability in the periphery may no longer come as a surprise as AI can predict where political stability is breaking down…or where a humanitarian crisis is beginning to brew, giving existing institutions early warning that stability is in peril thereby allowing an earlier response. Tracking migration, human trafficking and international crime will likely be more productive when aided by AI.

Working Group 6: Training and Leader Education

Chair: **Kate Hansen Bundt (Norway)**

Secretary General, Norwegian Atlantic Committee (TAG)

Co-Chair/Rapporteur: **Lars Frølund (Denmark), Lecturer,** Massachusetts Institute of Technology (MIT) **(Confirmed)**

The Training and Leader Education Working Group discussed how foreseeable threats, challenges, and scenarios of 2035 and the changing character of war (based on defence and security implications of emerging and disruptive technologies) will affect national and NATO training and leader education. How should leaders (e.g., policymakers, senior defence and military leaders, commanders, acquisition and resource managers), individuals and units be trained, educated, and developed to best ensure the development and employment of future capabilities, and the execution of future warfare concepts (e.g. Multi-Domain Operations)? What tools are needed for future, realistic training, exercises (at scale), and leader education (e.g., AI and extended reality tools, enhanced modelling and simulations, improved digitization and ICT...)? What kinds of future scenarios should be used to train senior policymakers and military leaders to understand future threats and challenges and how best to counter them with strategies and capabilities? How can interoperability between allies, between allies and partners best be achieved through training and leader education? How can training and leader education improve civil-military cooperation and synchronisation for resilience, hybrid threat and crisis response, deterrence and defence? How can NATO ensure the right subject matter expertise needed in its civilian and military staffs and military command and force structures to plan, prepare, and respond to future war, including leveraging emerging and disruptive technologies and developing future concepts? What kinds of fellowships, internships, and exchanges should be implemented to enhance talent and leader development across NATO civilian and military bodies?

Joanna van der Merwe (Netherlands), Fellow, Centre for European Policy Analysis

Peter Watkins (UK) Visiting Professor, King's College London

Tomonori Yoshizaki (Japan), University of Tokyo

Gisela Stuart (UK), Chair, Wilton Park

Mick Ryan (Australia), Mick Ryan Leadership (TAG)

THE REPORT

1. Recommendations

The group is of the opinion that Training and Leadership Education is crucial for the competitiveness of the Alliance. It is therefore the recommendation of the group that:

1. Professional development in Defense and Security should consider the concept of a “Total Defense” scenario in a poly-crisis and comprise 4 main categories: 1) Command leadership and ethics, 2) Joint warfighting/multidomain war fighting, 3) Strategy and Policy, and 4) Technology and capability.
2. Institutions in Defense and Security should define and clearly communicate what they require in terms of skills, knowledge, and experience at all ranks/grades (and, preferably, by individual posts). They should properly resource the learning and professional development process with time, money and personnel. The institutional leaders – at the time - must own the whole process and advocate for it on behalf of their institutions (stewardship).
3. The equivalent of 2,5 % of national security and defense budgets should go to professional development (including education and leadership development) [this figure is analogous to UK national target for expenditure on R&D]. The 2,5 % for professional development should be counted towards each country’s contribution to meeting the NATO commitment to spend at least 2% of GDP on defense.

2. Core message

> Defense and security institutions need a more accessible, continuous, personalized, and adaptable learning culture to gain and sustain an intellectual edge over competitors and adversaries.

3. The What, the Who and the How

The following describes the WHAT, WHO and HOW of the way defense and security institutions can get to have a more accessible, continuous, personalized, and adaptable learning culture to gain and sustain an Intellectual edge over competitors and adversaries.

THE WHAT

We consider four categories of skills and knowledge that are needed – to a greater or lesser degree – at all levels of command and leadership in defense and security (full list, please see the annex A):

1) **Command, leadership and ethics** – this category include important areas such as "The Theory of Leadership Development", "Ethics", "Principles of Command", "Self-awareness and empathy", "Group Dynamics", "Principles of Command", "Command and Control", "Doctrine Development and Adoption", "Organizational Learning", and "Military and Civilian Planning".

2) **Joint warfighting/multidomain war fighting** - this category includes important areas such as "Military and Civilian planning", "Command and Control", "Logistics", "Intelligence", "Deception and operational security", and "Stakeholder management"

3) **Strategy and Policy** - this category include important areas such as "Strategic Communication", "Organizational Change and Innovation", "Alliances", "Finance and Budget Planning", "Defining Policy Objectives and Follow-up", "Organizational change and innovative culture", "Strategic thinking and building a vision",

"Understanding institutional frameworks", "Strategic workforce planning" and "Resilience with a focus on expecting the unexpected".

4) **Technology and capability** - this category include important areas such as "Technology Adoption and Scaling", "Risk Capital and Entrepreneurship", and "National Resilience", "Project management and evaluation", "Tech literacy", "Conventional military development of new technologies", "Cybersecurity", "Force modernization process", "Workplace Safety and security", and "National resilience".

THE WHO

Importantly, we believe that the emphasis placed on each of these four categories – which collective is the core curriculum – should be adapted in the professional education at five different levels in their careers: Initial, Junior, Middle Manager (and military equivalent), Senior, Institutional leaders, and finally Political leaders. The table below illustrates (with 1 = High Emphasis and 4 = Low Emphasis) how we consider the right emphasis of the four categories for each career level. As an example, we believe that the Junior Manager will need to focus predominately on Command Leadership and less on Technology and Capability at this point in their career whereas the Senior Leader will focus predominately on "Strategy and Policy".

WHO	1) Command leadership and ethics	2) Joint multi-domain war fighting	3) Strategy and Policy	4) Technology and capability
Initial	1	2	4	3

Junior	1	2	4	3
Middle Manager	1 (STATEGY-BRANCH) 2 (TECH-BRANCH)	4 (STRATEGY-BRANCH) 3 (TECH-BRANCH)	2 (STRATEGY-BRANCH) 4 (TECH-BRANCH)	3(STRATEGY-BRANCH) 1 (TECH-BRANCH)
Senior	2	3	1	4
Institutional Leaders	2	4	1	3
Political leaders	3	4	1	2

THE HOW

We have identified several challenges in the current form that Professional development is delivered in the defense and security community. The critical challenges we believe are that Professional Development is 1) too time consuming and with too much time away from home/work, 2) not taking into advantage personalized, adaptable learning technologies (which leads to a very slow further development of the curriculum), and 3) is still very nation centric meaning that there is no cross-learning between allied nations.

Instead, we believe that Professional development need to be 1) radically adaptive and personalized and thus taking into account where people are in their learning, 2) should be implemented with an ‘entire government approach’ with a specific focus on the development of the ‘mid-career core’, 3) clearly linked to institutional promotion, incentives and desired behaviors.

Working Group 7: Ethics and Legal

Chair: Professor Nigel Biggar (UK), Regius Professor, Moral and Pastoral Theology, **University of Oxford**

Co-Chair/Rapporteur: Professor Paul Schulte (UK), University of Birmingham **(TAG)**

The Ethics and Legal Working Group addressed how international rules and codes governing the conduct and limits of warfare, including international humanitarian law and rules of engagement, might have evolved by 2035? What principles of responsible use should NATO adjust or develop to account for the future employment of emerging and disruptive technologies (e.g., AI, autonomy, big data and ICT, hypersonic systems, space-based technologies, quantum technologies biotechnology and human enhancement)? How can NATO become a leader in the development of ethical concepts related to future technology and warfare? What other bodies and stakeholders (industry, academia, civil society) should NATO engage in the development and adjustment of principles of responsible use and other ethical and legal concepts? How should policymakers, capability developers, military commanders, staffs, and operators be trained and educated to ensure employment of future capabilities according to principles of responsible use and other ethical and legal concepts?

David Whetham (UK), Professor of Ethics and the Military Profession, King's College London, London, United Kingdom

Marina Miron (Germany), Post-doctoral researcher at the War Studies Department, King's College London,

Rachel Kerr (UK), Professor of War Studies and Society, King's College London

THE REPORT

I. Core message

1. NATO has good reasons to agree and promote ethical norms and guidelines about the military uses of new technologies. However, the present prospect of winning consent from Russia, China, and the Global South to new international law is not promising. So, while seeing what can be done to create diplomatic common ground for a new international treaty and considering how the new technologies might enhance its own compliance with current International Humanitarian Law, NATO should focus on strengthening agreement on norms among its member-states and using its market-power and liaison with professional bodies to promote them worldwide. In addition, it should support the relevant education of senior decision-makers.

General considerations

2. Military ethics is not about preventing or hamstringing the use of lethal force. It's about controlling it. Why should NATO want to control it? So that it serves our purpose, rather than subverts it. What is our purpose? To defend a humane and liberal way of life. We cannot do that if we choose to defend it by military means that make us inhumane and tyrannical. So, we need to control our use of lethal force.

3. Moreover, the call for a statement of ethical norms and guidelines about the use of novel technologies is coming from within the military itself. The publication of norms by military institutions serves to relieve the uncertainty of individuals, and thereby to enhance military efficiency and alacrity.

4. Further still, NATO will be held to stringent ethical account by critics at home and abroad. How well NATO answers its critics will help to determine how much political opposition its actions arouse. Political opposition can create military problems.

5. A basic issue is that NATO's adversaries seek to extend and promote a less humane and illiberal way of life, and that they are therefore less inclined to constrain their military means. That may put NATO at a disadvantage in the deployment of the new technologies. Does that destine to defeat? Not necessarily. Technological superiority does not always prevail in war. Sometimes its advantages are overwhelmed by non-technological—say, political—weaknesses. Thus, the technologically superior West lost the war in Afghanistan. And it is not clear that Russia's present atrocious lack of restraint in Ukraine has given it a significant military advantage. It might have cost it diplomatically in causing its failure to get returned to membership of the UN Human Rights Council. Besides, suffering humane constraints, and cleaving to the moral high ground, will be necessary for NATO to maintain the support of domestic electorates and technology company workforces—although popular scruples may relax in an existential conflict, as they did among the British in the Second World War.

6. Of course, if it were to persuade the rest of the world to sign up to an international law that subjects them to the same constraints, NATO might not suffer any disadvantage. Diplomatic efforts should be made, therefore, to try and build common ground on which a new law might be agreed. However, right now the prospect of persuading Russia and China, or even the Global South, to agree to a treaty seems bleak. And even if they did sign up, we might well find their practical interpretation of the law dramatically different from our own.

7. However, even if NATO cannot expect to lead the world by causing the rest of the world to follow it—it has internal reasons to agree among its members humane and liberal ethical rules to control its own use of military technologies. What should these be? This is not the place to work through each of the new technologies, identify the ethical issues it raises, and decide on suitable rules. However, we can say that there seems no need to develop novel ethical and legal criteria. The familiar, long-tested ones will suffice: for example, moral responsibility and accountability regarding Artificial Intelligence (AI) and autonomous weaponry; proportionality and discrimination regarding responses to cyber-aggression; informed consent regarding human augmentation; and open-eyed, realistic prudence regarding the limitations and risks of bright new shiny technology in general.

II. Outlying thought

1. While there is often very good reason to want to respond faster than the enemy—say, to an incoming missile attack—we should be careful not to assume that maximum speed is always desirable and confers a military advantage. After all, doing something stupid faster than your opponent does not advantage you.

III. Recommendations

2. At least for the sake of its own military cohesion, NATO's member states should continue to strive toward greater agreement on the rules governing the use of the new technologies. An obvious, straightforward **first** step would be a collective reaffirmation that all new technology adapted by NATO should conform to international law.

3. **Second**, NATO should consider how the new technologies might enhance its own compliance with current International Humanitarian Law—for example, through more precise targeting and better intelligence.

4. Lots of unilateral work is already going on within member-states. A **third** obvious step would be to collect all this for discussion, perhaps agreement, at NATO level.

5. While getting agreement on common values is difficult, it is not impossible. Take the case of the military uses of Human Augmentation. National positions are emerging that are not consistent with each other. However, bodies like the Multinational Capability Development Campaign led by the US, which seeks to encourage common standards and approaches among NATO allies and partners, has published a set of agreed 'common considerations' that are broadly compatible with the positions of all member states. A **fourth** step would be to add to these and refine them over time as technologies—and dialogue about them—mature.

6. Adding in normative requirements late to mature technology is challenging, slow and expensive. However, right now member-states do not disagree very dramatically about the principles and operational rules governing the military uses of Artificial Intelligence. A **fifth** step would be to formulate these rules as an agreed set of requirements, so that the commercial producers of defence-related technologies would take them into account at an early stage and incorporate them efficiently into their products at minimal expense. Given the need for new technology companies to maximise their market, setting a required minimum specification for the NATO one would probably shape the way technology is developed. In this way, NATO as a whole could use its power as a major global consumer to wield world-wide ethical influence in shaping norms.

7. This is in fact the approach already being taken by the UK regarding the military uses of AI. The agreed higher-level principles are currently being specified and explained at the operational level, so that there is a clear expectation of what 'human-centricity' means in relation to a new sensor-system employing Human Machine Teaming. That expectation will then appear as a requirement in any tender process.

8. Many emerging military technologies require professionals to be involved with their use or deployment. These include medical personnel, engineers, scientists, some in uniform, some not. But whether military or civilian, all of these are subject to professional codes of conduct. These codes comprise powerful norms that shape behaviour and therefore the application of new technology. A **sixth** step, therefore, would be for NATO to engage with international professional bodies so that military considerations are taken into account in the development of professional codes and best practice—for example, with regard to neuro-enhancement and human machine-teaming.

9. For example, the Institute for Electronic and Electrical Engineers is the leading international, non-governmental, professional organisation covering all things related to electrical engineering. In the field of neuroscience, it has sponsored multiple international working bodies seeking to understand the implications of applying a common set of bio-ethical principles in different sectors, ranging from telecommunications and media through to the military. The military working group comprises international scientists with direct experience of working with military organisations around the world. While direct input might not be appropriate, NATO could still influence this enterprise in professional norm-generation indirectly, since some of the IEEE scientists also work with some of its own institutions such as the Defense Advanced Research Projects Agency (DARPA). In the long run, shaping the professional expectations of best practice is likely to affect actual behaviour.

10. A **seventh** step concerns not the development and promotion of international norms regarding the military uses of the new technologies, but the education of political leaders about them. At least senior civil servants, and perhaps even their political masters, could benefit from taking short Continuing Professional Development courses designed to bring senior decision-makers up-to-date on the new technologies and their military applications. For example, King's College London, the University of New South Wales, and Arizona State University are developing just such courses in the specific area of AUKUS technologies (nuclear, submarine, AI, hypersonics, etc.) and their implications—ethical, social, and political.

IV. Summary

11. In sum, our recommendations are that NATO should: (1) affirm its commitment to comply with international law; (2) consider how the new technologies might enhance its own compliance with current International Humanitarian Law; (3) gather together unilateral work for collective discussion and perhaps agreement; (4) develop the MCDC's 'common considerations'; (5) formulate agreed rules re. AI as a set of NATO requirements of technology producers; (6) liaise with professional bodies about the formulation of codes of conduct vis-à-vis the military uses of the new technologies; and (7) support the education of senior decision-makers about such uses.

Working Group 8: The "Dreadnought Working Group

Chair: Dr Bryan Wells (UK), NATO Chief Scientist

Chair/Rapporteur: Anna Wieslander (Sweden) Director, Northern Europe**, Atlantic Council** (TAG)

The Dreadnought Working Group considered the impact of combinations of emerging and disruptive technologies on military strategy. According to NATO Science and Technology Trends 2023-2043 the most likely impactful combinations include: Data-AI-Autonomy, Data-AI-Biotechnology and Human Enhancement, Data-AI-Materials, Data-Quantum Technologies, Energy-Materials-AI, Space-Hypersonics-Materials, and Space-Quantum. What kinds of impact on defence and military strategy and policy will these combinations of EDT have? What combinations of EDTs are potential adversaries focusing on and how best should NATO and nations respond to defend against them? What kinds of capability development strategies and approaches are needed for NATO and nations to leverage and protect the potential of these combinations of EDT to retain NATO's military advantage?

James Holland (UK), Writer, Broadcaster and World War Two Historian

Lawrence Freedman (UK), Emeritus Professor of War Studies, King's College London

Paul Beaver (UK), Director, National Spitfire Project

Rob Bertholee (Netherlands), former Commander, Royal Netherlands Army (TAG)

Rob de Wijk (Netherlands), Founder, Hague Centre for Security Strategy (TAG)

Yves Boyer (France), Emeritus Professor, Ecole Polytechnique

THE REPORT

The core task for the Dreadnought Working Group was to consider the impact of combinations of emerging and disruptive technologies on military strategy, using the Dreadnought as a point of departure. The group discussions therefore initially circled around the basic questions; What was the Dreadnought? How is it relevant today as a metaphor and as a historical example?

In short, the HMS Dreadnought was a Royal Navy Battleship, which entered into service in 1906. The design of the ship revolutionized navy power, and because of its capabilities were so advanced, it led to a whole generation of battleships being associated with it. It was equivalent of two or even three ships before her. This of course took enormous efforts and vast expenses over many years. The Dreadnought had supremacy in speed, range, agility, the size of the guns and its destructive power – all of this resulted in military dominance. It was built in secrecy, which was unusual at the time, and the Germans were in shock and panic when it was launched.

The Working Group used the term *Dreadnought* as a metaphor for a strategic military shock.

The Working Group then chose to work with two scenarios which were two sides of the Dreadnought coin: either (i) NATO and Allies face a Dreadnought threat from Russia and/or China, or (ii) NATO and Allies could benefit from a Dreadnought Moment of their own by successfully developing such a capability. A Dreadnought moment could be a new weapon system, which the group mostly discussed, but the group also acknowledged that the Dreadnought could be thought of in a wider sense, for example the US leaving NATO, or finding the synthetic substitute to a rare earth mineral crucial for new technology.

Two sides of the Dreadnought coin

A. Dreadnought upon us – (Pearl Harbor moment)

How do we deter? Or rather, is it possible to deter?

There are many elements for successful deterrence in a Dreadnought context.

Deterrence can be undertaken partly through large *exercises*, thereby showing resolve and strength. NATO could do more pop-up presence and snap exercises, hence playing on ambiguity to strengthen its nuclear deterrence posture.

Intelligence assessment is a key element. Allies have to make sure that they do not have gaps in intelligence, and there should be a sufficient level of intelligence sharing among allies. NATO can also work actively with joint threat assessments. There is a risk that NATO and Allies assess the intelligence incorrectly, particularly if the conclusion is uncomfortable. For instance a large-scale Russian-Chinese exercise and troop mobilization somewhere along the Eastern flank might be incorrectly assessed. NATO and Allies might not therefore be able to see the Dreadnought moment coming. Equally, NATO and Allies would have to prevent the adversary from using the Dreadnought: *deterrence-by-denial* is the best. Understanding and navigating the political context is necessary to successfully calibrate the appropriate response.

The group discussed the example of Pearl Harbor, which was an intelligence failure, and concluded that NATO and Allies would need to demonstrate that they have long term *resilience*, including the basic infrastructure, ammunition, manpower and people who understand why they are fighting; it is in the nature of the psychology of a shock that civil society will adjust.

Mobilisation is an important instrument, but there would be particularly difficult political decisions on the point in a crisis escalation at which mobilization was activated. In addition, readiness of troops is insufficient in many allied countries and a major weakness in NATO's New Force Model. The *total defence* concept is useful, but in some countries like the UK there is no total defence framework, which makes it more difficult and increases the risk that the an ally is taken by surprise.

Allies need to engage in *strategic communication*, such as conversations with the public on the threats from Russia, China and other adversaries. There is a need to counter disinformation and propaganda and explain why Allies must invest more in defence and preparedness.

At the moment, NATO and allies rely heavily on *nuclear deterrence* which is insufficiently constructed. NATO would put the nuclear weapons on alert to deter when a Dreadnought moment approached or occurred, but NATO lacks missile launch systems for nuclear weapons in Europe. It is a vulnerability that Europe is dependent on aircraft in such a situation as the F35's do not reach far enough.

How do we defend?

Selected proportionality would be the guiding principle. The West would wish to avoid escalation in the case of a Dreadnought moment being brought upon us. We should not assume that we would respond symmetrically.

The *industrial base* is central. Allies have industry, a strategy, and funding but there needs to be political will to scale up and enter wartime production rates. The European Defence Industrial Base will have an important role.

The technological challenge will be how to *mature technology into a capability* as rapidly as possible will be t. Ukraine has been quick at improvising, driven by existential threat perception, which is an inspiration to us all.

B. Our Dreadnought moment

What would we want to achieve?

There are four elements that impact on what we would want to achieve with a strategic military capability shock: capability demonstration; political will to sustain the capability; technical considerations on developing the capability; and Allies working together.

Capability Demonstration

We would need to *demonstrate* that we have the technological capability of a Dreadnought (this need not be expensive)

We would wish to create a new layer of deterrence in order to defend every inch of NATO territory and provide a broadened, pro-longed escalation ladder which would provide politicians with more options along the road of handling war or crisis, in between traditional conventional and nuclear options (in order to prevent using them).

How do we gain political will?

Dreadnought is not only about technology: human factors are important and above all the *political context* must be considered. There needs to be a sense of urgency, of threat, and NATO Allies are split when it comes to existential threat perception. The big powers do not sense it. For a Dreadnought moment to occur for NATO and Allies, urgency must be combined with boldness. Put differently, leadership is a prerequisite.

Once the Dreadnought is in place, it is possible to create NATO buy-in and transparency by creating a group like the NATO Planning Group which deals with nuclear weapons.

Technical considerations

How would we identify Dreadnought? The most likely combination would be Data-AI-Autonomy which could be an intelligent unmanned air platform consisting of a combination of 6th generation F35s accompanied by powerful drones. Such a platform could for instance deliver and protect nuclear bombs at a completely new level.

The technology comes from commercial actors which means that we need well-functioning channels from civil tech companies to the defence companies and R&D establishment.

- Industrial strength in turn requires:
    - Manufacturing capacity. The European Defence Industrial Base is important.
    - Finance. Defence expenditure, the 2 % being floor not the ceiling.
    - Manpower. Tech expertise, logistic support.

How would allies work together?

To develop a Dreadnought moment, allies should team up in smaller numbers, for instance the Nordic States could collaborate together. Another example is AUKUS, with its second pillar focusing on cooperation on new technologies. The basis for collaboration would be shared interests and costs. NATO and Allies do not focus sufficiently on production.

Recommendations

If NATO has a Dreadnought (strategic shock) capability, NATO and allies should:

- Be clear what they want to achieve:
    - Broaden the ladder of escalation before the nuclear threshold is reached. (Identified as a gap)
    - Enhance ambiguity towards the adversary, through complexity of responses available.
    - Make our decision making simpler but the adversary's more complex.
    - Enhance resilience.
- Establish the necessary political will to act and invest: "Wake up, get ready, take action!"
    - Note that different Allies have different threat perceptions. They also have different strategic cultures. Both need to be bridged.

    - Allies need to undertake significant strategic communication to their own public and potential adversaries about the threat and need for resolve and investments to address it.
    - Nations need to act as an Alliance to provide credibility and legitimacy.
- Nations need to address elements other than technology.
    - Manufacturing capacity. The European Defence Industrial Base is important.
    - People: Tech expertise, military, logistic support.
    - Materials, including critical raw materials, rare earth minerals. Stockpiling necessary.
    - Concept of Operations (CONOPs): how we would actually use the Dreadnought in our operations.
    - NATO and allies should reinforce the use of AI in scenario exercises using best practices from elsewhere.

Recommendations: Deterrence and Defence against a strategic shock

NATO and allies should:

- Recognize that strategic shock often arises from incorrect intelligence assessment and therefore improve intelligence sharing and assessment among individual allies (not NATO collectively) – this is possible when there is a shared interest. There should be greater red teaming of assessments by using AI/computing.
- Enhance resilience using Total Defence concepts, fulfilling NATO's baseline requirements on resilience and ensuring alignment with the NDPP. The risk of unrest/uprisings as reactions to potential use of nuclear weapons should be addressed by engaging civil society,
- Start considering asymmetric responses – creating unexpected combinations of responses with difficulty of attribution, massive cyber attacks, attacks on satellite systems, hitting for instance internet, banking, food and water supplies, and create our own Dreadnought moment.
- ensure flexible response options. For the military, long range delivery systems, conventional and or nuclear, are needed. Nuclear weapons are our strongest response and that instrument needs to work better in order to be credible.

Final Group reflection:

An interesting conclusion is that new technology is just one element that is necessary for military strategy. Rather, technology needs to be seen as part of a broader civil/military system if it is to be decisive. As with nuclear weapons, EDT combinations could indeed help deliver strategic military shock, but they need to be incorporated into a wider system in order to be effective.