Report

The Future War and Deterrence Conference

Monday 3 – Wednesday 5 October 2022 | WP3052

With sponorship from:

With additional support from:

Wilton Park

Report

The Future War and Deterrence Conference

Monday 3 – Wednesday 5 October 2022 | WP3052

In partnership with The Alphen Group and with major funding support from NATO, sponsorship from Improbable Defence, Helsing, UK Foreign Commonwealth and Development Office with additional support from Airbus Defence and Space, BAE Systems, NATO Defence College and Premise Data

"If you want things to stay as they are, things will have to change"

Giuseppe Tomasi di Lampedusa

Wilton Park and The Alphen Group jointly organised this three day, invitation only conference on future war and deterrence, bringing together over 60 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 six working groups – affordability and resilience, future force, policy, industry and innovation, strategy and technology. These groups met for the entire second day of the event (the conference programme can be viewed below). They constituted the key mechanism for delivering the conference outcomes, focused primarily on how to achieve enhanced deterrence of state on state conflict projected out to a horizon of 2035.

Following the main findings and recommendations below, the report takes up the conference proceedings, beginning with the opening plenary sessions that set the context for the working group deliberations, including lessons from the war in Ukraine. The report then summarises the outcomes of the six working groups. Appendices contain the full working group reports.

Main Findings and Recommendations

1. By 2035, everywhere will be a battlefield and everything will be a weapon. The Ukraine War has shattered hope for peace that has existed since the end of the Cold War and the fall of the Berlin Wall. The post-Cold War world has come to a crashing end. There is now an urgent need for clarity concerning so-called 'red-lines', not only over possible use of nuclear weapons, but cyber warfare, information warfare and the use of emerging and disruptive technologies across the defence, information, military and economic (DIME) space.

2. Emerging and disruptive technologies entering the battlespace could revolutionise warfare by 2035, at the very least profoundly change the character of war. Whilst Russia is the immediate threat the danger Moscow poses is a consequence of decline and an inability to adapt to the twenty-first century. Instability in many parts of the world must also be engaged. Going forward China poses the greatest systemic threat due to a combination of great and developing economic and military power, an autocratic leadership that divides the world into adversaries and client-states, and rapid technological advance that is fuelled by industrial, cyber and military espionage. China's rapidly ageing population is reinforcing Beijing's technology drive across the information, military and economic domains. China and Russia must be systematically prevented from accessing defence sensitive programmes, including dual-use technologies. Far greater efforts need to be made collectively to block Chinese and Russian industrial and cyber espionage.

3. Deterring future war starts with properly learning the lessons from the war in Ukraine, particularly in Europe. There is a tension between rhetoric and reality across the conflict spectrum, poor integration of policy and effort across diplomacy, information, military and economic domains, and little consensus or even idea about how to proceed either nationally or collectively.

4. Maintaining sufficient threat-led defence investment will prove difficult going forward because of pressures on many sectors of society and due to the structural economic challenges the democracies face caused by the financial and banking crisis, the pandemic and the war in Ukraine. If democracies are to deter future war, leaders will need to understand and appreciate the value of defence and not just its cost, and communicate that to their respective populations.

5. Preserving a just peace and effective deterrence is the core business of the democracies in general, and NATO in particular. Deterrence will continue to be centred on conventional and nuclear forces but must be reinforced by a new concept of deterrence that stretches across the hybrid, cyber and hyperwar mosaic.

6. The speed of decision-making will also need to be far faster if deterrence is to be founded on the speed of relevance because of the increasing prevalence of Artificial intelligence (AI), machine-learning, quantum computing, loitering strategic glide systems, deep strike hypersonic missiles, intelligent and unintelligent drone swarms, and nanotechnologies. Ambiguous hybrid attacks, while low-tech, can also compress decision-making and complicate threat assessments in a fast-moving crisis

7. By 2035, at the very latest, Europeans will need a high-end, first responder force that can act from sea-bed to space and across the domains of air, sea, land, cyber, space, information and knowledge. A force of sufficient size and twenty-first-century manoeuvre to be able to respond to any threat from the Arctic to the Mediterranean with predominantly European capabilities should the US be engaged in strength elsewhere and unable to provide its full complement of reinforcements. A force also of sufficient mass to simultaneously support front-line Allies in dealing with significant regional crises and insurgencies.

8. The impact of decisive new technologies on strategy and doctrine will lead to profound changes in the character if not the nature of war. The Allied future force must be built on and around the enabling technologies that are entering and shaping the battlespace. The true test will be interoperability with the US future force in 2035 at the high-end of conflict and under extreme duress.

9. Ultimately, if future war is to be deterred, deterrence itself will require a profound re-imagining of statecraft with deeper synergies forged between policy, strategy, civilian and military forces and resources together with a new balance between power projection and people protection. Such synergies will be critical for the future functioning of the Alliance but must be extended to all the democracies in what is a global emergency. Now is the moment to begin constructing such an architecture because the future peace will demand nothing less.

10. Future war and deterrence is not simply a question of technology. Democracies today are facing complex strategic coercion via applied disinformation, deception, destabilisation, disruption and the threat of actual destruction. Democracies thus face a potential *Dreadnought* moment and digital decapitation through a combination of hybrid and cyber attacks allied to new technologies being applied to devastating effect by enemies against vulnerable, open societies.

11. China is "tomorrow's fight" and Russia the immediate fight, even if Moscow is degrading its conventional military capabilities rapidly. Together, China and Russia have embarked on a systematic strategy to exploit American weaknesses and vulnerabilities both before a conflict and in the event of conflict. Such measures include interfering with the American political process and seeking to exploit US military over-stretch. China is in a "waiting game" with the democracies, with Beijing firm in its belief that in time the "correlation of forces" will favour China where its vital interests are at stake – Taiwan and much of south-east Asia. Russia's decline means Moscow knows it has no time to waste.

12. There are now apparent limits to the scale of US engagement in NATO even if the Americans remain fully committed politically to "defending every inch" of Alliance territory. US military overstretch is being exacerbated by European military weakness even though efforts are being made at mitigation through the more equitable sharing of burdens and risks within the Alliance, along with the reaffirmation at the 2022 Madrid Summit of all aspects of the 2014 Wales Defence Investment Pledge.

13. A culture of worst-case planning and exercising must again be established. In any major future war the democracies could face multiple simultaneous contingences via a series of global 'feints' across technical domains and in the Indo-Pacific, Middle East, Black Sea, Arctic and Europe.

14. If NATO's new Forward Defence posture is to be credible, European allies (plus Canada) will need to take on far greater strategic responsibility. At the very least it will require a profound change in the culture, capabilities and capacities of European forces, their supporting strategic enablers and especially the political mind-set of leaders. Above all, Europeans must plan to be in the lead in and around Europe in a pre-war emergency and the opening phases of war itself. They should also have the expeditionary forces needed to become the first responders to most crises along Europe's periphery.

15. There is a gap between NATO's conventional military deterrence and the nuclear deterrent which has lost all or any tactical application and thus increasingly lacks credibility as a deterrent against Russia's "escalate to de-escalate" strategy. There is a pressing need to revisit NATO's nuclear posture and command and control mechanisms to ensure the deterrent is sufficiently agile and proportionate to the threat. Dual-capable systems are in urgent need of modernisation.

16. A new and far more interactive and proactive partnership is needed between government, defence industries and the wider military supply chain. Such supply chains also need to be made more robust and secure. The pace and scale of political, economic and military-technical change risks undermining Allied cohesion and force interoperability, as well as keeping security and defence planning in democracies off-balance, with long-term project management a particular lacuna.

17. Acquisition cycles are far too slow, with acquisition of platforms in Europe taking on average 5-7 years whilst technology evolves every 5-7 months. As the war in Ukraine is demonstrating, European states in particular simply lack the defence industrial capacity to ramp up production immediately and rapidly. A strategy is needed that would be akin to something like the British Shadow Industry Plan of 1935, which enabled London to rapidly increase war production in 1939. It would need to be Alliance-wide and involve the entire supply chain, with procurement and acquisition processes adapted accordingly to improve fielding times of both platforms and systems.

18. Defence investment, particularly in future tech, will require both the reform of the respective defence and technological bases that empower new democratic partnerships and with it a far greater willingness to share technologies. To that end, the European Defence and Technological Industrial Base (EDTIB) in particular must become far more coherent, co-ordinated and greatly reformed to markedly improve the quality, availability and fielding of vital equipment.

19. There are seven domains of future war – air, sea, land, cyber, space, information and cognitive/knowledge. They are all equally important as pillars of credible deterrence and the conduct of future war. The information war will be pivotal. Intelligence-sharing needs to be expanded and accelerated to properly underpin future deterrence because data generation, sharing and devolution down mission command chains will be critical in future war.

20. Allies and Partners together need to develop a technology strategy built on a common technology picture if the integration of sensors and shooters—vital in the future OODA loop (Observe, Orient, Decide, Act) — is to underpin the acceleration of effect and response (hyperwar) that will be needed for applications of AI, super/quantum computing, satellite technology, big data crunching, drone tech, hypersonic systems et al.

21. The NATO Defence Investment Pledge must be seen as a baseline rather than a goal (a floor rather than a ceiling). Only then will the future force that Europeans and other democracies need be realised by 2035. Such a force will be expensive because it will need to include a mix of existing systems-integrated empowered platforms data-fused with new strategic enablers across the multiple domains of air, sea, land, cyber, space, information and knowledge. Mass and manoeuvre in the NATO area of responsibility will depend on rapid force generation, much faster and more robust command and control, much enhanced strategic lift (sea and air), autonomous but embedded ISTAR, electronic warfare and other future tech capabilities with the aim of breaking into an enemy's OODA loop whilst protecting that of the Alliance.

22. The use of machine-enabled systems and robotics in future war requires an urgent debate about the ethics and place of the human decision-maker in the command and kill chain. By 2035 technology could be sufficiently advanced for decisions of attack and defence to be decided autonomously if not independently by machines. Given that speed of command will be the speed of relevance and that enemies might not have the same commitment to ethical controls, the future of deterrence will depend on such a balance.

Proceedings

Introduction

1. The Future War and Deterrence Conference considered war and peace in 2035. Its primary reflection was how to maintain strategic stability and thus prevent a systemic war by ensuring deterrence remained credible out to the year 2035 and beyond. To that end, there were six themes which were reflected in the six working groups: affordability and resilience, future force, innovation and industry, policy, strategy and deterrence, and technology. The question this working conference addressed was what if deterrence fails? Evidence would suggest it could be the beginning of a catastrophic long war that in a relatively short period would reach across the hybrid, cyber and hyperwar (super-fast) spectrum of conflict. The working assumption was that any such war must be prevented through enhanced and strengthened deterrence.

2. Hard choices and radical solutions are now needed together with a new partnership between political leaders, practitioners, industry and experts to ensure recent decisions to increase defence investment are maintained and properly implemented as part of a longer-term strategic view of deterrence and defence to 2035 and beyond.

3. The core assumption in much of the debate was that only the US will be able to guarantee Europe's defence and deterrence going forward, and reinforce those of Partners in the Indo-Pacific, if Europeans and Partners develop (and quickly) the resources, resilience, but above all sufficient fighting power to act as high-end first responders in an emergency and act as part of a new security partnership of global democracies.

4. The current crisis is a consequence of a series of crises that have afflicted the world since 2008, destabilised the international system and seen a shift of power and wealth away from Western democracies towards China in particular. However, the same crises have also de-stabilised China, and particularly Russia, increasing the likelihood of military adventurism as the autocrats in both countries seek to maintain power. That shift has been exacerbated and exaggerated in the West by false assumptions about globalisation, a political culture, particularly in Europe, that favoured the impression of power rather than the fact of it, as well as long and unsuccessful campaigns in both Afghanistan and Iraq.

The Challenge

5. The post-Cold War interbellum is at an end and the time for self-delusion with it. By invading Ukraine, Russia has embarked on a struggle with the West that could continue for many years. China is also determined to challenge the American-anchored rules-based international order. Consequently, the United States will only be able to guarantee the security and defence of Europe going forward if Europeans do far more for deterrence and their own defence due to the overstretch the two autocracies are imposing on American armed forces. Both the EU and NATO are beginning to address these challenges with the EU Strategic Compass and the 2022 NATO Strategic Concept. However, the level of ambition of both falls significantly short of what will be required to re-establish the credibility of deterrence in a fast deteriorating, changing and increasingly contested global strategic environment of which Europe is only a part and for which meaningful partnerships with other democracies will be vital, most notably, Australia, Japan and South Korea.

6. 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, information and knowledge. A force of sufficient twenty-first 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 Partner in dealing with significant insurgencies and emergencies. A force built on and around the enabling technologies that are entering and shaping the battlespace: artificial intelligence (AI), machine-learning, quantum computing, loitering strategic glide systems, deep strike hypersonic missiles, intelligent and unintelligent drone swarms, and nanotechnologies. The true test will be interoperability with the US future force and those of Partners in the Indo-Pacific at the high-end of conflict and under extreme duress.

7. A new balance will also need to be struck between platforms and systems. Western democracies still spend too much money on “unpolished platforms” and assume restricted warfare. Chinese exercises suggest Beijing is rapidly moving towards a new military concept of unrestricted warfare reinforced by integrated asymmetry by adopting a system of systems approach. Drones will be a particularly important component of any arsenal and will come in many forms and provide many services, giving an attacker a critical advantage in the battle space. By 2035, robotic warfare could well be on the way to complete autonomy on the battlefield, posing both multi-dimensional command opportunities and challenges, even triggering a potential collapse on the battlefield. Totally autonomous drone swarms will become the norm with so-called ‘Banshee’ drones operating randomly and following non-linear trajectories to fulfil their tailored missions. Existing platforms will be transformed by retro-fitting them with AI systems based on data-fusing, which was tested at the 2022 TF59 exercise.

8. The NATO Madrid Summit and the 2022 NATO Strategic Concept renewed the focus on collective defence as the Alliance’s primary core task together with crisis management and co-operative security. It also prioritised resilience. One of the major challenges facing the Allies is that much of the ‘muscle memory’ of the Cold War has been lost and the Alliance in particular no longer has many of the skills or expertise to exploit many of the lessons that still have value from that era. Therefore, new architecture needs to be erected that will embed the Alliance’s future policy and strategy direction in the high-end challenge. With Finland and Sweden joining the Alliance it will be vital to ensure NATO’s new longer front can be protected, Russia deterred, the US equitably supported and deterrence re-established as the Alliance’s core mission. For that to happen there needs to be a level of Allied and Partner ambition built on three premises: firstly, the Alliance is already engaged in a war that is implicitly existential; secondly, NATO is not a global alliance, but exists in a global context; thirdly, robust political cohesion and military interoperability with Partners such as Australia, Japan, South Korea and other democracies will be vital to NATO’s core mission and must be focused on use and development of a range of NATO Standards. They have been developed over 75 years and will be the glue in future coalitions.

9. The next twelve months for NATO will be as critical as any the Alliance has been through in its now long history. Whilst many of the Alliance’s challenges are technological, technology is not the salient problem, rather it is adaptation and maintaining progress in the adaptation of NATO’s Military Instrument of Power (MIOP) to the new strategic environment. NATO forces must “be ready to go and keep going” but such ambition requires the Alliance to follow through with its efforts to become capable across the multi-domains of air, sea, land, cyber, space, information and the cognitive/knowledge. An Alliance that is markedly more capable in space and cyber-space is particularly important if NATO is to “maintain the military edge” with a specific focus on continuous adaptation and transformation of the NATO Force and Command Structures to meet the needs of the warfighter. By 2030 at the very latest, NATO must be able to conduct multi-domain operations. At present, the Alliance is still unable to process the mass of data such a mission-suite will require, a problem that afflicts most democracies. The digital transformation of command structures will be particularly important, the NATO Command Structure to the fore, but it will require both political cohesion and robust and sustained political will.

10. The Madrid Summit was a “prise de conscience” but how long the window of opportunity for the robust adaptation and renewal of Alliance military structures remains open is a moot point given the many other social and economic pressures the Allies are under. Madrid agreed to change NATO’s force posture to enhance deterrence and defence from the Barents Sea to the Black Sea. A New Force Model was also agreed together with a new “family of plans”, both of which are designed to strengthen NATO’s Article 5 commitment and thus deterrence. A new planning cycle was established for the NATO Defence Planning Process (NDPP) with a marked upward shift in the Alliance’s level of military ambition to reinforce Article 5 contingencies across the multi-domain environment, reinforced by increased defence investment and both a renewed Warfighting Concept and a Deterrence Concept. It was also agreed that the Alliance will field more high-end warfighting capabilities with a particular focus on reinforced Integrated Air and Missile Defence (IAMD), deep strike capabilities, and modernised and far more agile land forces, all of which will be better integrated across the multi-domain environment.

11. Deterrence is the core business of both the Alliance and Allies/Partners, with the singular aim to convince all and any adversary, whether alone or in concert with others, that an attack on the Alliance of the wider Community of Democracies would simply not be worth the risk. A new concept of deterrence is also required, built on a balance between enhanced people protection, societal resilience and power projection. Allied deterrence will still be centred on NATO’s conventional and nuclear forces even if a more elaborated nuclear capability is needed across the tactical, theatre and strategic spectrum as a matter of urgency, and Allies must accept their nuclear deterrent responsibilities. ‘Traditional’ deterrence must now be reinforced by information deterrence and cyber deterrence, including the capacity for offensive action.

Lessons from the war in Ukraine

Headline: Western deterrence failed prior to the Ukraine War because Russia did not believe, or refused to believe, that the democracies would impose a heavy price if Moscow crossed a red-line and invaded Ukraine. This failure of deterrence began in Syria in 2013 and in Crimea in 2014. Deterrence must never fail again. The attritional nature of the war has revealed the danger of sacrificing significant mass to afford a little manoeuvre.

12. Russia and the invasion of Ukraine pervades all sixteen pages of the Strategic Concept, which has a marked change of tone compared to its 2010 forebear. The 2010 Strategic Concept described Russia as a ‘strategic partner’, even though Russia had invaded Georgia two years prior in 2008. The 2022 Strategic Concept is far less equivocal. “The Russian Federation’s war of aggression against Ukraine has shattered the peace and gravely altered our security environment. Its brutal and unlawful invasion, repeated violations of international humanitarian law and heinous attacks and atrocities have caused unspeakable suffering and destruction.” Allies and Partners must respond accordingly with sustained and consistent support for Ukraine and to reinforce Alliance deterrence and defence.

13. The war in Ukraine is a test of wills, not only between Russian and Ukraine, but also Russia and the West. Moscow is at war with all the democracies, and for all the tragic and murderous incompetence of their conduct of the war the democracies must assume the Russians are preparing for a long struggle and that they will have Chinese support.

14. It is vital Allies and Partners communicate systematically and consistently to the Russians that there are ‘red lines’ that if crossed could lead to war with the Alliance and that Moscow’s actions have reinforced the determination of the Alliance to fulfil its deterrence and defence mission. NATO’s Military Strategy and deterrence and defence posture must thus be purposively linked to a new escalation ladder that stretches across the hybrid, cyber, and hyper war (conventional and nuclear) force spectrum.

15. There are already lessons from the war in Ukraine that can be drawn about the future force, the most pressing of which will be the need to better use technology to authorise action at the lowest level possible of mission command. Flat-line command and control structures have enabled Ukrainian forces to avoid decapitating Russian strikes of the command structure. In some respects, land warfare has become like submarine warfare as Ukrainian forces have proved very adept at concealment, stealth and sudden strike. The war has also seen a shift towards Über-targeting" based on the principle of small-unit action and the best-placed unit given command authority to strike at their discretion. The Russian force and command structure has at times become unhinged by such actions and kept almost permanently off-balance.

16. European and Partner forces will need more robust logistics forward deployed, with enhanced and far more secure military supply chains particularly important. Far more materiel is also needed, most notably ammunition. If deterrence and defence are to be credible Allies will also 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. Deployed NATO forces will need much improved force protection, including through reduced detectability and thus digital footprint of force concentrations ('bright butterflies').

17. The war in Ukraine has revealed as well 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 space. Enhanced land-based, protected battlefield mobility will be a core requirement 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.

18. Moscow's use of hybrid warfare must generate a proportionate and co-ordinated Allied and Partner response, with Russia's many vulnerabilities exploited, particularly the personal interests of the elite who control the Kremlin. A systematic analysis of Russia's many civilian and military vulnerabilities is thus needed.

19. Strategic communications is an essential element of deterrence. Messaging should focus on Russia's many military weaknesses such as vulnerable force concentration, static and insecure command and control, the massive digital footprint, poor battlefield mobility etc., allied to sufficient force deployed forward to create doubt in the mind of the Kremlin that any further or future military adventure could succeed at a price acceptable to them. This could also include the vulnerabilities of Kaliningrad, the Northern Fleet, and Russian forces in Syria.

20. 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 some kind of twenty-first century equivalent of the Maginot Line, secure pre-positioned capabilities and access to individual ready reserves will also be vital.

Summaries of key working group findings and recommendations

Affordability and resilience

Headline: Russia is a long-term threat. Direct threats to Allies and Partners cannot be discounted. Affordability and resilience are thus inextricably linked. Resilience needs to be re-cast in light of Russia's brutal behaviour and Moscow's willingness to weaponise energy, food and other commodities, whilst analysis of affordability tends to focus too much on 'traditional' areas.

21. Affordability must include burden-sharing with no NATO nation having to bear more than 50% of the cost of the Alliance. Resilience has become an increasingly broad concept in the wake of the financial and economic crises, pandemic, climate change and the war in Ukraine.

22. In the wake of the 2022 Madrid Summit NATO is taking steps to accelerate adaptation and improve burden-sharing by increasing the role of European Allies in providing for their own deterrence and defence, by conducting more exercises, and by increasing the role and importance to the Alliance of Partners such as Australia, Japan, South Korea and others.

23. If Future Force 2035 is to be affordably realised industry's role will be need to significantly increase, and whilst it will remain independent of policy must become more closely intertwined with it.

24. For the purposes of sound defence planning a precisely drawn concept of resilience is required with a focus on protecting the home base against all and any effort to coerce, threaten, intimidate or attack. Such measures would be specifically focused on strengthening critical vulnerabilities in areas such as transportation, communications, infrastructure, energy and information.

25. Far more systematic and sustained efforts must be made to promote synergies between the EU and NATO as part of a new resilience strategy. Allies should enhance protection of those resilience categories within which an adversary would most intend to exploit vulnerabilities to facilitate covert or open aggression. These threats focus primarily on communications and energy nodes, critical infrastructure, continuity of government, cyber defences, military mobility-related transportation nodes and societal susceptibilities to disinformation and propaganda. The future NATO-EU partnership should focus on such threats.

26. NATO Security Investment Programme (NSIP) projects and initiatives provide "value added" to allies in key resilience domains such as cyber defence. NSIP funding should be at least doubled to keep pace with on-going increases in allies' defence spending, consistent with the Defence Investment Pledge and to provide needed extra resources in these key resilience domains. Other specific actions that could be taken now include ensuring that funding of the NATO Certified Instructor Programme (NCIP) is doubled to keep pace with defence spending so that the information and knowledge domains are also strengthened.

27. Critically, the 2% GDP defence investment per annum of which 20% must be spent on new equipment must now be seen as a baseline rather than a ceiling. The NATO Defence Planning Process must also be adapted to exploit a range of low-cost technologies within the framework of the 2019 Military Strategy.

Future Force

Headline: Fighting power in 2035 will be 24/7 in a constantly contested, boundless, persistent and cross-domain battlespace from sea-bed to space and from cyber to cognitive. Therefore, Euro-Atlantic Allies and Partners in the Indo-Pacific should work collectively on a paradigm for the future force that is focused on high-end threat-based operations reinforced by host nation support.

28. NATO strategic ambition and military reality must become far more aligned. The Military Strategy is centred on SACEUR's Area of Responsibility (AOR) wide Strategic Plan (SASP) and the Concept for the Deterrence and Defence of the Euro-Atlantic Area (DDA). There are two main pillars; the NATO warfighting cornerstone concept (NWCC) and the Deterrence Concept. The New Force Model at the heart of the Strategic Concept is the consequence of the Military Strategy and it is there one finds the necessary detail. This detail specifically includes the call for the enhanced NATO Response Force of some 40,000 troops to be transformed into a future force of some 300,000 troops maintained at high alert, with 44,000 kept at high readiness. For the first time all rapid reaction forces under NATO command will be committed to a deterrence and defence role and all such forces will be consolidated within one command framework. Whilst the new force will be held at 24 hours 'Notice to Act' the bulk of the NATO Force Structure will held at 15 days 'Notice to Move', which will be a marked improvement over the current structure in which some forces are at 180 days' notice to move.

29. At American behest the new force will be mainly European with Allies on NATO's Eastern and South-Eastern Flanks agreeing to expanded deployed battalions to brigades of between 3,000-5000 troops. Allies must follow-through. For example, the British have two battlegroups deployed to Estonia which they now wish to draw down in spite of having committed to deploy an additional battlegroup.

30. The Forward Defence strategy will also see heavy equipment pre-positioned near NATO borders. A force of that size and with the necessary level of fighting power would normally mean that with rotation there would always be a force of some 100,000 kept at high readiness, which will be extremely expensive for NATO European allies grappling with high inflation and post-COVID economies. A NATO standard brigade is normally between 3200 and 5500 strong. Given that both air and naval forces will also need to be included a land force of, say, 200,000 would need at least 50 to 60 European rapid reaction brigades together with all their supporting elements. At best, there are only 20 to 30 today. There are already concerns being expressed by some Allies.

31. Going forward the Future Force must be integrated by design, with far fewer, smaller and more technologically-advanced headquarters. The Military Strategy also implies a return by NATO, and by extension Partners, to fundamental principles of war with a concept of military victory further informed by lessons from the Cold War. Vital synergies will include the merging of the NATO Command Structure and the NATO Force Structure to ensure far better agility and cohesion driven by threat-based strategy across the seven domains of air, sea, land, cyber, space, information and knowledge.

32. The Military Strategy is the first such strategy since 1967. The aim is to empower the commander to deliver effect wherever and whenever required through far greater exploitation of information technology. This change in the way NATO does military business will reinforce the importance of the Joint Force Commands in Brunssum and Naples but likely with fewer Combined Air Operations Centres (CAOC).

33. Going forward the architecture of the future force will require much greater systems integration between hardware and software and enabling of existing platforms, many of which will still be in service in 2035. The future force will need to balance concentration of force and the number of deployed headquarters with the need to disperse. To that end, European ambitions, capabilities, capacities and the funding that supports them, both for Allied and national operations, will need to keep pace with the US to ensure continued American support for NATO and to keep pace with evolving threats from China and Russia.

34. The new NATO Family of Plans, with the 2019 Military Strategy at its core, can both provide the framework going forward and ensure interoperability through shared standards with Partners in the Indo-Pacific. The future force will have limited mass, even though its exploitation of future technologies will enable it to generate the effects of a much larger force of today. Enabling technologies will thus be crucial to the high-manoeuvre warfare of the future. And, whilst technology will reduce the presence of humans in the command and kill chain it is vital that industry work closely with armed forces to simplify the use of advanced technologies under duress in the battlespace.

35. Technological advances will require careful management to ensure commanders are not overwhelmed with either information and/or decisions at crucial points during battle. Therefore, it is vital the human and organisational aspects of force modernisation are properly considered, along with the need to avoid a technology fetish, so that speed and precision are maintained at all times and in all circumstances.

Innovation and industry

Headline: Success goes to those states that prioritise the speed of delivery and to that end see industry as part of the defence structure. As the war in Ukraine is demonstrating European states in particular simply lack the defence industrial capacity to ramp up production immediately and rapidly. A strategy is needed that would be akin to something like the British Shadow Industry Plan of 1935, which enabled London to rapidly increase war production in 1939. It would need to be Alliance-wide and involve the entire supply chain with procurement and acquisition processes adapted accordingly to improve fielding times of both platforms and systems.

36. In the twenty-first century deterrence is built on technological and industrial strength. A defence-industrial strategy must be built on trust between Allies, Partners and industry, combined with early and deep involvement in establishing requirements and specifications. Such trust is particularly important as the pace, change and scope of emerging and disruptive technologies is 'de-synchronising' the acquisition process for platforms, systems, data and information. Future force requirements will likely require skills and technologies from beyond the defence supply chain and involve far more small and medium enterprises (SMEs). 'Big marquee' programmes can act as a barrier to such involvement due to their complexity, and also increases costs and slows down delivery and fielding times.

37. Far closer client-supplier relationships must be established as part of a 'life-cycle partnership' to ensure the procurement model is far more agile and meets the needs of a specific requirement and its timely delivery. Wholesale adoption of partnering processes should be examined together with long-term skills development within the client community. This will ensure all parties to procurement have far more "skin in the game".

38. To realise future force ambitions Europeans need a European Defence and Technological Base (EDTIB) that is compatible and competitive with those in North American and Indo-Pacific Partners. Above all, industry must once again be seen as an 'instrument of state'. Current threat-driven ambitions will not be delivered unless the current EDTIB is transformed, in particular industry/customer relations.

39. Political interference and the link between national defence policies and industrial policies act as a constant drag on efficient and effective procurement and acquisition. Without radical change defence innovation will continue to be blocked by narrow national and sectional interests. NATO's Committee of National Armaments Directors (CNAD) must be transformed into a procurement hub in conjunction with the European Defence Agency (EDA). No longer can competition for programmes be reduced to the lowest compliant bid.

Policy

Headline: Policy goals can only be crafted from a proper understanding of the emerging security environment and the political vision and determination to respond proportionately and appropriately. Policy assumptions of all democratic governments drive and reflect both the level of ambition and the willingness to share the wider security and defence burden as part of a common effort. Too many policy stovepipes continue to exist. Policy cohesion will be vital if the ends, ways and means of future deterrence are to be demonstrably credible.

40. A NATO-Plus Concept is needed to build trust between political and military leaders via an "informed strategic dialogue" and exercises that test accelerated decision-making in the pre-war. During the Cold War ministers regularly took part in major exercises, playing themselves. It is time to return to such practices to ensure early and sustained devolution of command authority in a pre-crisis emergency so that decisions can be made at the speed of relevance. This is important not least because even by 2035 it is unlikely that devolved command authority will extend to bespoke operations.

41. Sound policy and the assumptions that support it are as much an element of credible deterrence as capabilities and capacities. Given the likely speed of command of future war, deterrence and defence will require decision-making able to act at the speed of relevance. A new balance between political leadership and military authority will thus be needed both immediately before war breaks out and during hostilities.

42. A twenty-first century version of the All Arms Battle will still pose a challenge for democracies given the need for urgent decision-making in crises and immediate decision-making in war. Many such authorisations are already included in the NATO Crisis Response Manual, but the problem of early agreement remains a potentially critical obstacle. One major challenge will be the degree of devolved command authority to give to military commanders, most noticeably Supreme Allied Command, Europe (SACEUR), who already enjoys significant discretion to act from the North Atlantic Council.

43. The first step must be to clearly understand what command authority SACEUR already possesses and what is still needed. One option to further speed up decision-making could be to install SACEUR as a permanent participant in the North Atlantic Council (NAC) by 2035, with the NAC-SHAPE relationship effectively virtual. NATO-Plus should also include like-minded Partners who must be closely involved in all political consultations with mechanisms in place to realise such synergy and cohesion. Critical civilian actors will need as well to be deeply immersed in contingency planning and exercising as part of what will be little short of a "comprehensive deterrence and defence concept". NATO will inevitably be at the core of such a mechanism because it is the world's most experienced and advanced pol-mil hub and the guardian of NATO Standards.

44. In 2035, China and Russia will be the main autocratic adversaries of the free West and deterrence will need to have the policy, strategy, force and resource in place commensurate to deterring the threat. There will be a host of other potential adversaries both in the Indo-Pacific and Middle East and North Africa that are enabled with relatively cheap but empowering technologies. NATO will have implemented the Madrid Summit decisions and thus will be forward deployed with 50% of all NATO capabilities necessarily European given the pressure US forces will be under.

45. The Alliance must be in a position to robustly respond to any threat of incursion or invasion and the Military Instrument of Power (MIOP) must be fully-equipped, with sufficient forces held at an appropriate level of readiness and mission command reinforced by education, exercising that tests to fail, and training. The Alliance will also need to be in close active partnership with democracies the world over to establish effective and efficient deterrence across the hybrid war, information war, cyber war, and conventional and nuclear hyperwar.

46. Partners in the Indo-Pacific should be invited to work with the Allies to develop compatible strategic outlooks based on agreement over shared red-lines to be communicated to friend and foe. Much of that future relationship will be built on expanded intelligence-sharing and the capacity to share data rapidly, securely and easily, possibly through initiatives such as the Five Eyes intelligence community and AUKUS. A shared programme of exercising and war-gaming should be designed forthwith. Many of the democracies are still on a peacetime footing but will need to ensure their respective security and defence institutions are on a war footing, with NATO to the fore. Much closer relationships between NATO and like-minded Partners in the Indo-Pacific will act as a force multiplier.

47. One of many challenges will be the need for democracies to maintain an ethical approach to the use of AI and other technologies at the operational level even if learned machines are permitted to make some decisions at the tactical level. One way forward would be to consider how autonomous, intelligent strike systems might be programmed to respect international humanitarian law. All the democracies need to consider such challenges together.

Strategy and deterrence

Headline: credible deterrent strategy in 2035 will require full spectrum deterrence. Whilst much of the effort will be focussed on the Military Instrument of Power not every threat will be linked to war. Therefore, a new concept of deterrence is needed that is more graduated and extends across statecraft, information, energy, cyber and all aspects of the military domain, both technological and geographical. The credibility of future deterrence will rest on an adversary believing that the democracies mean what they say and have the necessary capabilities and capacities. Ukrainian success would already markedly strengthen deterrence.

48. At its most challenging, the strategy OF deterrence will need to be credible in the eyes of near-peer competitors and equal to the threat posed by intense strategic competition. Given that China and Russia will be the main challengers, strategy will need to prevent a war on two fronts simultaneously – in Europe and the Indo-Pacific.

49. Much of the strategy will require a balance between diplomatic, informational, military and economic (DIME) engagement. In dealing with China and Russia, whilst the focus will necessarily be the non-military aspects of statecraft, both diplomacy and economic, it will not be credible unless underpinned for force that is sufficiently credible in both Beijing and Moscow.

50. Military deterrence will thus need to be credible across a broad spectrum of conventional, unconventional and nuclear force. It will also require the application of active and passive deterrence and both deterrence by punishment and deterrence by denial with coercion, deterrence and containment re-established much as they were during the Cold War.

51. European Allies, in particular, urgently need to re-learn how to merge such measures into an escalation ladder that is credible and robust even in a crisis. Indeed, a re-examination of Alliance practice during the Cold War would afford the Allies both a precedent and experience for the hardening of policy and strategy that credible deterrence will require.

52. Deterrence and resilience will also need to be closely linked. There are a range of measures that could be implemented in the short-term, such as preventing Chinese acquisition of technology companies. Best practice partnerships should also be deepened between the democracies to deter unconventional cyber and digital attacks and to make political systems more robust in the face of interference. Best practice should also be sought to ensure that social resilience is an element of sound deterrence.

53. Critically, the gap between conventional force and nuclear force deterrence needs to be closed. Russia has been constructing a range of treaty-flouting short-range and theatre-based nuclear systems with relatively low yields and which they are now threatening to use on Ukraine. As many European conventional forces have become relatively weaker the nuclear deterrents of the US, Britain and France have become ever more strategic. An adversary needs to know that catastrophic responses are still afforded democratic leaders in the event of an attack. Whilst the conventional-nuclear gap must be closed the response need not be symmetrical. Offensive cyber capabilities could go a significant way to offsetting such weaknesses.

Technology

Headline: Artificial intelligence (AI), machine-learning, quantum computing, loitering strategic glide systems, deep strike hypersonic missiles, intelligent and unintelligent drone swarms, nanotechnologies and a host of other emerging and disruptive technologies will revolutionise the battlespace by 2035 and beyond. How and to what extent? Above all, the democracies needs to be far more aware of the possibility of revolutionary breakthroughs to avoid a Dreadnought moment. There is a pressing need for political and military leaders to better understand both the pace and breadth of technological change. Whilst the United States will be central to technological innovation and application, all the democracies need to work in harness to best apply emerging and disruptive technologies to deterrence and defence.

54. An independent variable is the reason a change occurs in a dependent variable. In 1906, Britain launched the first all big gun, more heavily armoured and faster battleship than any other afloat – HMS Dreadnought. At an instant she made every other capital ship obsolete, including squadrons of the Royal Navy. However, most policymakers and practitioners do not really understand the implications and applications for such technologies in the battlespace.

55. Emerging and disruptive technologies will be the independent variable in the future war and deterrence mix. It is not clear to what extent they will 'emerge' and to what extent they will really disrupt. However, the conditions do exist, at least potentially, for a Dreadnought moment in which a technology, or a combination of technologies, leads to a decisive, albeit inevitably temporary change in the character of war.

56. This is not just an issue of technology but rather the combination of technology with speed over distance. The Ukraine War might have emphasised for a time at least the dominance of the defence over the offence, but the scale, pace and change of technology would suggest the opposite by 2035. Unfortunately, policymakers and commanders fail to properly understand the nature of the new technologies, their scope or their application, partly because the pace at which such technology advances and partly because they were born into an analogue age. Technologists love the potential of their technology and the theoretical applications it might have in strengthening deterrence, but they rarely understand force. Politicians and policymakers vaguely hope it will lead to a step change in capability as well as offset a lack of capacity. They further hope that the digital will achieve all of the above far more affordably than the traditional analogue as the life cycle of platforms becomes ever longer simply because they are precisely that – platforms for systems because technology and systems integrators are advancing far faster than metal bashers.

57. At the very least, emerging technologies will require the involvement in the defence supply cycle of companies and enterprises for whom defence is at best a side-show. It will profoundly change the relationship between customer, prime contractor and sub-contractor. These changes are necessary if the defence sector is to be an area of business activity in which many tech companies would want to engage.

58. The current defence supply cycle is simply too slow and orders too little over too long a time to be attractive to many technologists who have the capacity to greatly empower the offensive and defensive capabilities of the major democracies. That is the one thing that is clear about the otherwise 'sci-fi' relationship between emerging technology and future war. The other thing that is clear is that the state that masters the relationship between force, resource and technology will be the world's dominant military power in 2035.

59. Whatever happens, autonomous, intelligent firepower is going to increase exponentially by 2035, together with the need, perhaps, for an eighth cognitive domain. To establish a proper defence planning understanding of the mix of technologies that will be best applied there will also need to be a "re-combatting of innovation", i.e. innovators will need to be attracted to solving military problems. That is because their mission will be to combine ultra-high speed (hyper speed) with high lethality at the high end of warfare and ensure allies and partners can operate together.

60. Unless an Ally can operate at the speed of relevance to, say, the US future force, would such forces be seamlessly interoperable? Or, could technology afford the solutions across a spectrum of interoperability by automatically optimising economy, effective application and efficient use of all forces available to a commander at any given time? Across the military domains mission command will be more not less important than today because technology will promote disaggregated and devolved command structures.

61. Data and its fidelity will be a core component of deterrence and defence going forward, not least because of the centrality of data to effective command and control. Control and management of resilience and response will also be a critical factor primarily because each component of the OODA loop is accelerating due to technology. Acting will be increasingly AI-driven, and whereas in the past the intention of an adversary informed any counter-action technology will simply not consider intentions. Rather, algorithms will 'decide' the most efficient course of responsive action in any given circumstance.

62. Deterrence is already being eroded by technology and decision have to be taken now if emerging gaps are to be seen to be closed. Future deterrence will also need to adapt at the speed of relevance. Given the centrality of technology to such adaptation only a bespoke and hardened strategic public private partnership between government, industry, science and technology will suffice. Such a partnership will be particularly important if the human core component in both deterrence and defence is to be enabled by technology, not replaced by it. Having more scientists engaged in both policy and strategy will be important.

63. Over time, arms control will need to be rehabilitated as part of a broad approach to confidence-building and risk-reduction. Technologies will be key to verification of new arms control regimes. As Russia's strategy in the continuing war in Ukraine continues to evolve and potentially escalate, its attempts at nuclear intimidation and coercion could bring a return of intensified demands from elements of our societies for arms control, risk reduction and a negotiated peace. Russia will exploit these concerns by offering one-sided and unbalanced arms control and conflict resolution offers.

64. Specific actions that should now be taken include legal reforms that can reinforce deterrence, including the cross-border movement of forces and dangerous goods. Endurance must also be reinforced with a particular focus on the space domain to prevent denial of critical services and information. A far more effective interface between government and intellectual capital also needs to be forged.

David Richards and Julian Lindley-French
Wilton Park | October 2022

Appendices

Conference Programme

MONDAY 3 OCTOBER

1300 Participants arrive and buffet lunch available – informal dress.

1445-1500 Welcome and introduction:

General the Lord Richards of Herstmonceux, Former UK Chief of Defence Staff
Dr Robert Grant Programme Director, Wilton Park
Professor Julian Lindley-French Chairman, The Alphen Group

1500-1630 Session 1: Future war and deterrence 2035 – a vision

This plenary will look out to 2035 and offer a vision of future war and deterrence and help establish the likely level of policy ambition that is now required to realise such a vision.

Professor Julian Lindley-French
Dr Amir Hussein CEO, Spark Cognition
Angus Lapsley Assistant Secretary General for Defence Policy and Planning, NATO

1630-1700 Tea/coffee

1**700-1730 Session 2: Keynote address**

Virtual intervention by Hologram* General Philippe Lavigne Supreme Allied Commander Transformation (SACT), NATO *10 mins presentation followed by 20 mins Q&A

1730-1845 Session 3: Future war and deterrence including lessons from Ukraine and other recent conflicts.

This plenary session will frame the work of the conference and the working groups by considering relevant lessons from the war in Ukraine and a number of other recent state on-state conflicts as well as the direction of travel of future deterrence and war.

Professor Tomonori Yoshizaki Director, Policy Simulation, National Institute for Defense Studies (NIDS), Japan
Virtual intervention LTG (Ret.) Ben Hodges Co-author Future War and the Defence of Europe, and former Commander, US Army Europe.

1900 Reception followed by dinner with speakers from defence industry sponsors

TUESDAY 4 OCTOBER

0800-0845 Breakfast – formal civilian dress for photograph and conference dinner (ties can be removed during working groups)

0900-1030 Session 4: (working groups session one) – mission, work plan & opening discussions.

1030-1100 Tea/coffee

1100-1230 Session 5: (working groups session two) – discussions

1230-1330 Lunch (including Working lunch meeting for Chairs and co-chairs of working groups plus command group in conference room)

1330-1430 Premise Data, Improbable, Helsing show and tell or free time

1430-1600 Session 6: (working groups session three) – discussions

1600-1645 Photograph followed by tea/coffee

1645-1815 Session 7: (working groups session four) – preparation of main point report to plenary and main points for conference rapporteur.

1815-1845 free time

1845 Reception followed by formal conference VIP dinner (Sponsored by Premise Data) Hosted by General the Lord Richards of Herstmonceux. Keynote address by Admiral Sir Tony Radakin, Chief of Defence Staff, London

WEDNESDAY 5 OCTOBER

0800-0845 Breakfast and checkout – informal dress.

0900-1100 **Session 8. 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.

1100-1130 Tea/coffee

1130-1140 Evaluation survey Completion of online survey

1140-1300 Session 9: Future war and deterrence – the way ahead.

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.

Dr Bryan Wells Chief Scientist, NATO
Baroness Gisela Stuart Board member, Royal Navy Strategic Studies Centre; Chair, Wilton Park
Concluding discussion
Final remarks General the Lord Richards of Herstmonceux

1300 Lunch

1400 Participants depart.

Full working group findings and recommendations

Affordability and Resilience Working Group

Principal Recommendations

- Allies' resiliency and allied deterrence are inextricably linked. In the face of Russia's full-scale aggression against Ukraine, both need to be significantly enhanced. Each is expensive, and warfighting capabilities and resilience enhancements compete for resources among many other demands on national treasuries. As a result, affordability considerations must take account of more than simply the cost of the capabilities needed to implement agreed military strategies.
- The decision by NATO Leaders at the 2022 Madrid Summit to re-endorse in its entirety the Defence Investment Pledge (DIP) from the 2014 Wales Summit should be expeditiously fulfilled, as many allies are now moving out smartly to do. That said, two adaptations should be made. Firstly, 2% of GDP should be considered as minimum defence spending (i.e., as a "floor") and separate from spending on enhanced societal resilience. Secondly, lower cost technologies should be exploited to address the full range of threats as NATO now acts to operationalize the 2019 NATO Military Strategy through the Deterrence and Defence of the Euro-Atlantic Area (DDA) strategy and the NATO Warfighting Capstone Concept (CWCC).
- In considering affordability, fair burden-sharing remains essential. No Ally should be expected to field more than 50% of any specific capability. National development of 'niche' capabilities can add to deterrence, but it must not be at the expense of a broader set of capability requirements that every ally should be reasonably challenged to provide.
- Allies should enhance protection of those resilience categories within which an adversary would most intend to exploit vulnerabilities to facilitate covert or open aggression. These threats focus primarily on communications and energy nodes, critical infrastructure, continuity of government, cyber defences, military mobility-related transportation nodes and societal susceptibilities to disinformation and propaganda. The NATO and EU partnership should be intensified to prioritize these threats.
- NATO Security Investment Program (NSIP) projects and initiatives provide "value added" to allies in key resilience domains, such as cyber defines. NSIP funding should be at least doubled to keep pace with on-going increases in allies' defines spending consistent with the Defence Investment Pledge and to provide needed extra resources in these key resilience domains
- As Russia's strategy continues to evolve, and potentially escalate, in the on-going war in Ukraine, its attempts at nuclear intimidation and coercion could bring a return of intensified demands from elements of our societies for arms control, risk reduction and a negotiated peace. Russia will exploit these concerns by offering one-sided and unbalanced arms control and conflict resolution offers. NATO and the EU, both collectively and as individual members, must be prepared through intensified public information and public diplomacy efforts to explain why these offers cannot be accepted. The diplomatic and political engagement "pillar" of the 1967 Harmel Report strategy remains important, but Russia must halt its aggressive behaviour and comply with international law if such engagement is to produce mutually acceptable and beneficial outcomes.
- For the foreseeable future we must assume Russia has malign revanchist intent, manifested in a range of threats up to and including direct aggression towards NATO Allies. As stated in the 2022 Strategic Concept: "We cannot discount the possibility of an attack against Allies' sovereignty and territorial integrity."

Background, Context, and Discussion

Under the Chair of Dr Robert Bell and Co-Chair Brigadier (Ret.) Robbie Boyd, panellists Ann Lundberg, Gisela Stuart, Mark Hoffman, and Paul Schulte participated in a Working Group (WG) to examine the affordability and resilience dimensions of future war and deterrence. Our most important and relevant observations are summarized in this report.

In the context of deterring and if needs be winning a major state-on-state war in 2035, the WG considered how best the dimensions of affordability and resilience can reinforce deterrence credibility, given competing demands for national public finances. We were aided in this task by the fact that earlier this year against the reality of the major war that is on-going in Ukraine, the EU and NATO have each produced major strategic guidance documents that look across the strategic landscape at least a decade into the future. For the EU, that is the Strategic Compass agreed in late March. For NATO, that is the Strategic Concept agreed in late June in Madrid. This new overarching Alliance strategic guidance was significantly informed by the NATO Military Strategy that had been agreed by Chiefs and Heads of Delegations (CHODs) in 2019. That strategy is comprised of two components: SACEUR's Concept for the Deterrence and Defence of the Euro-Atlantic Area (DDA) and the 10–15-year threat-based horizon scan led by SACT, the NATO Warfighting Capstone Concept (NWCC). We noted that military advice from the Military Committee at CHODs level had led to a subtle yet important strategic philosophical change in NATO military strategy from a capability focus to a threat focus, particularly from Russia and China. We have, therefore, examined what we think NATO and the EU got right and what more may be required in these two areas.

Nations' affordability assessments tend to be focused on what is required to field traditional deterrence and defines capabilities, as was codified in the 2014 Wales Summit Defence Investment Pledge (DIP). The WG applauds the decision by NATO Heads of State and Government in the 2022 Strategic Concept to re-endorse the DIP in its entirety. The 2014 DIP includes the commitments by each ally to aim to spend by 2024 2% of its GDP on defines, from which 20% is to be invested in R&D and procurement programs – 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 NATO Defence Planning Process (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, there has been substantial progress amongst allies towards meeting the 2% minimum threshold, including notably from Germany.

That said, we believe two adaptations are necessary to the Pledge to take account of the current realities. First, the 2% goal must be seen as a minimum and separate from spending on enhanced resilience. Second, the application of these resources must also be tailored to exploit new lower-cost technologies and to operationalize the 2019 NATO Military Strategy. That includes both the DDA that guides SACEUR's planning for the "fight today" and SACT's NWCC for the longer-term warfighting vision, the "fight tomorrow". In addition, assessments of affordability must continue to incorporate the principles of "fair burden-sharing and reasonable challenge." No single ally should be expected to provide more than 50% of required capabilities in any specific domain. Role specialization should be encouraged where an ally has acquired important "niche" capabilities, but it should not be at the expense of its opting out of a broader set of capability contributions.

The WG discussions were underpinned by the principle that the Washington Treaty's Article 3 and Article 5 are in effect "bookends." Article 3 is in effect NATO's "resilience" clause, and Article 5 is its collective security "war clause" for crises where resilience and defines capabilities have failed to deter armed attacks from abroad. The more all allies are sufficiently robust in their resilience, the less the prospects that an armed attack from abroad might occur that would trigger a collective response under Article 5.

1. Percentage 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 Defence 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).

Article 3 states, "*In order more effectively to achieve the objectives of the Treaty, the Parties, separately and jointly, by means of continuous and effective self-help and mutual aid, will maintain and develop their individual and collective capacity to resist armed attack*." Hence Article 3 concentrates on resilience, including civil preparedness. As General Lavigne said in his remarks to the FWDC Plenary, "resilience is the ability of nations to recover from strategic shocks across critical vulnerability domains and respond." Resilience is first and foremost a national responsibility. Allies must be able to address the entire spectrum of crises envisaged by the Alliance.

The WG appreciates that the range of factors that underpin a nation's overall resilience is quite broad, extending from mitigation of climate change, to protecting against pandemics, to addressing large-scale refugee and asylum-seeking migrations, to promoting social and economic equity, and to countering terrorism and domestic populist extremism. We, however, have focused on enhancing protection of those resilience categories which an adversary would most intend to exploit vulnerabilities to facilitate covert or open aggression; for example, attacking or negating communications and energy nodes, critical infrastructure, continuity of government, cyber defences, or military mobility-related transportation nodes and targeting susceptibilities to disinformation and propaganda. Funding for resilience enhancements in many of these categories mostly does not come from defines budgets, and hence is not normally tied to NATO's affordability assumptions.

In addition, most of these categories involve EU competences, capabilities and resources. This means that the EU has the primary role in strengthening its 27 Member States' overall national resilience in political, economic and social domains. The EU clearly recognizes that Russia's aggression against Ukraine requires strengthening Member States' resilience across these domains. As the 2022 Strategic Compass states:

"We now need to ensure that we turn the EU's geopolitical awakening into a more permanent strategic posture. For there is so much more to do. The essence of what the EU did in reacting to Russia's invasion was to unite and use the full range of EU policies and levers as instruments of power. We showed that we are ready to pay a severe price to defend our security and that of our partners – the price of freedom. We should build on this approach in the period ahead, in Ukraine but elsewhere too".

This also means that the NATO-EU partnership should be intensified in building collective resilience in Europe, while NATO provides "value added" through NATO Security Investment Program (NSIP) projects to assist each ally in key domains (cyber defines, critical infrastructure protection, etc.) To achieve this, NSIP funding should be at least doubled to keep pace with on-going increases in allies' defines spending consistent with the Defence Investment Pledge. These extra resources could be applied, for example, to increasing the number of NATO Cyber Defence Rapid Reaction Teams that are available to travel to allies' capitals in the event of major adversarial cyber-attack, such as the devastating Russian cyber-attacks against Estonia in 2007. Such targeted investments would be consistent with the 2022 Strategic Concept's recognition that: "ensuring our national and collective resilience is critical to all our core tasks and underpins our efforts to safeguard our nations, societies and shared values."

NATO and the EU must have a horizon for assessing resilience requirements must extend to other regions, since we share common values, interests, and interdependencies with key partners in the Indo-Pacific, and competition from China is growing. NATO and the EU should enhance their interaction with key partners in this domain, recognizing, though, that resources must be prioritized for NATO and EU member states. Partners can benefit from NATO and the EU sharing best principles and agreed standards for resilience, if not financial assistance itself. Ukraine, though, is Sui genius – a special case in which Ukraine is for all intents and purposes fighting for European security in what increasingly is becoming a "proxy war" with Russia. As of September 28, the United States alone had provided Ukraine with approximately $19 billion since the illegal Russian annexation of Crimea in 2014, $16.2 billion of which has been delivered since Putin's full-scale invasion was launched on February 24 of this year. Other NATO and EU members, as well as regional partners, have contributed tens of billions more. NATO, EU Member States, and other Western partners must be prepared to continue to provide exceptionally high levels of military and financial assistance to Ukraine for some time to come, testing traditional assumptions concerning affordability.

Military efforts to defend Alliance territory, assets, and populations need to be complemented by robust civil preparedness, which should concentrate on continuity of government and essential services to the population as well as support for and to military operations. Civil and commercial sectors must be able to support military forces in areas that include transport (military mobility), communications, energy, basic supplies of food and water. NATO guides this through a Resilience Committee, which first met on May 19 of this year under the Chairmanship of Deputy Secretary General Mircea Geoana and reports to the North Atlantic Council.

We also believe the nature of resilience requirements will change as Russia's aggressive behaviour becomes more blatant and brutal. Where before resilience focused on protection against less direct hybrid or asymmetric "warfare," we now realize that Russia is prepared to engage in high-intensity conventional attack and, as its weakness therein are increasingly exposed, to escalate to the weaponisation of energy, food security, and nuclear power reactors and perhaps even direct nuclear weapons intimidation and possible use. The strategy of attempted nuclear coercion could bring with it a return of intensified demands from elements of our societies for arms control and risk reduction, and Russia may try to undermine our resilience with unbalanced offers that we will need to explain to our publics that cannot be accepted. The diplomatic and political engagement "pillar" of the 1967 Harmel Report strategy remains important, but Russia must halt its aggressive behaviour and comply with international law if such engagement is to produce mutually acceptable and beneficial outcomes.

Our WG concludes that for the foreseeable future we must assume Russia has malign revanchist intent, as may be manifested in a range of threats, including, as noted in NATO's Strategic Concept, the possibility of direct aggression against an Ally's sovereignty or territorial integrity.

Future Force Working Group Report

Shaping conditions

1. *NATO will remain the premier organizing institutional and operational structure for Western security. Other frameworks, however, such as the US Unified Command Plan and Combatant HQs, the UK-led Joint Expeditionary Force (JEF), the French-British Combined Joint Expeditionary Force (CJEF), the European Union (EU) and the UK-led Five-Power Defence Agreement (ANZUK) with Australia, Malaysia, New Zealand and Singapore will play important roles in coalition operations.*

2. *Defence of the Euro-Atlantic area is the defining requirement for NATO forces. It requires a capacity to concentrate forces and fires to counter Russian advantages. Defence in the Indo-Pacific region mandates a capacity to disperse forces and fires over long distances. Combining the two requirements will impose greater flexibility for NATO forces, such that they can operate within and beyond Europe, even if not under NATO command. At the same time, the United States is encouraging greater cooperation and force integration among Australia, Japan, Singapore, South Korea and Thailand, as a substitute for bilateral defence relationships that do not match new regional security dynamics. Therefore, there is today a greater degree of convergence between Euro-Atlantic and Indo-Pacific defence requirements from different points of departure. However, the latter will likely require more radical levels of innovation in the design of future forces.*

3. *NATO is an alliance of disparate nations, of varying size and military capacity. Future force structures will need to strike a balance that recognises geography between achieving military coherence and effectiveness, protecting political cohesion, and promoting multinational force integration and interoperability.*

4. *Future NATO forces will need to be able to perform collective defence, as well as crisis management and cooperate security, roles, along the peace-to-crisis-to-conflict spectrum, and across domains, based on modern advance plans.*

5. *Nuclear deterrence will remain an enduring shaping condition, but as part of a wider mix of capabilities in the missile defence, space and cyber domains.*

6. *NATO forces will continue to reflect a combination of new and legacy capabilities and face the challenges of combining them across over 70 separate armies, navies, air forces and special operations commands from 30/32 different nations.*

7. *Affordability and the burden-sharing imperative will remain major constraints in shaping the design, size and operational capacity of future force structures.*

8. *Evolution, rather than revolution, will remain the default option, because of competing missions, ever-present resource constraints, and technological uncertainties. However, on a case-by-case basis, revolutionary, non-linear solutions in the technological, doctrinal and force structure fields will probably yield high payoff advantages, particularly through the application of software (new technology) to hardware (legacy platforms).*

9. *To be effective, innovation will remain dependent on political initiative.*

10. *Engaging public opinion and securing public support will remain paramount*

Design drivers

11. The design of future forces on the scale of 30 (soon to be 32) Allies, with connections to several key Indo-Pacific partners, will require taking a broad “architectural design”, rather than a narrow “system engineering”, approach that balances a constellation of individual capabilities and a composite capacity.

12. This favoured “open architecture” approach (open, but still a recognisable design that all Allies can support) should help facilitate and support continuous adaptation. In particular, it should accommodate adaptable force mixes among nations; between high-end and lower-end forces; and across domains, recognising the challenges involved in achieving a genuine multi-domain operations capacity. Force compatibility and interoperability will be key factors.

13. Future HQ design should align with these factors, while aiming for a smaller number of headquarters across the NATO Command and Force Structures.

14. Future force design should integrate lessons from the war in Ukraine, notably in relation to command and control, electronic warfare and deep precision strike.

15. The design of future force structures will need to acknowledge the enduring impact of demographic constraints on recruitment and retention, while also recognising the limits of the substitution of personnel by technology.

16. Force structures should be understood as also encompassing the broader “infrastructure of defence”, from logistically-enabled itineraries for the movement of land formations and prepared air bases that support the relocation and dispersal of fighter and tanker squadrons, to fuel and equipment storage, ammunition stockpiling, Host Nation Support, and surge industrial capacity for the production of equipment items and munitions.

17. Lastly, future force structures must accommodate the requirement for higher readiness and responsiveness; strengthened operational capacity over longer distances and across domains; and the contribution of expanded levels of state-of-the-art and networked training, exercising and experimentation.

Industry and Innovation Working Group Report

- *A hiatus exists between inventors who know what they could invent, if only they knew what was wanted, and the soldiers who know, or ought to know, what they want, and would ask for it if they only knew how much science could do for them. You have never really bridged that gap yet. Winston Churchill 1941*
- *Success no longer goes to the country that develops a new fighting technology first, but rather to the one that better integrates it and adapts its way of fighting…our response will be to prioritize speed of delivery, continuous adaptation, and frequent modular upgrades. US National Defence Strategy 2018*

Headline: Industry is part of our force structure. We are dependent on industry to perform and, if we do not have a healthy industry, we do not have a healthy force. Frank Kendall Former US Under Secretary of Defence for Acquisition, Technology & Logistics 2012.

Core message

In the 20 years to 2021, the combined EU countries increased defence expenditure by 20%, the US by 66%, Russia by 292% and China by 592%[2]. Western nations and NATO need to relearn some of the 'national endeavour' lessons of industrial warfare – albeit contextualised for the information age – and provide the investment required to place their defence industries on a war footing. This needs to drive a closer and more transparent relationship between defence and industry to ensures that their forces can acquire and maintain the right information technology, combat platforms, support systems and munition stockpiles within the right timescale and at the right cost to deter and, if required, defeat future threats. The nature of 21st century warfighting technology suggests that industry must be an integral part of the through-life team that helps to maintain defence's combat edge and readiness.

Main themes of the debate

While still healthy, the West's demand-limited defence industrial base and S&T research and development (R&D) capacity are much reduced from previous eras of global confrontation. Notwithstanding testing counter-insurgencies, three decades of relative peace have led to the defence enterprise – strategic leadership, requirements and procurement staffs, and industry – being out of practice at sustaining larger numbers of more capable forces at higher readiness to underpin deterrence.

1. Maintenance of a strong S&T base and supporting investment are essential to sustain a warfighting edge; however investment can be wasted if key R&D activity is not exploited quickly. 'Spin-in' from adjacent (non-defence) sectors and incentives for S&T collaboration expand defence's ability to innovate. The pace at which ideas move from laboratory to frontline can be a deterrent in their own right; this relies on investment, focus and exploitation projects.
2. Defence requirements and procurement practice have yet to embrace fully data and information-centric capability: the platform remains King! This is not to eschew the importance of platforms; however they need to be better configured around the information [on-board or remote] operators need to fulfil their mission, and be able to integrate into a wider force.
3. Given that most equipment in service in 2035 is either in service now or is just coming into service, platform-based capability must accommodate faster refresh rates for information- and other sub-systems. There is some historical precedent for this and current experimentation in the field; HMS Dreadnought was a platform that fielded innovations that had been discretely developed independently for decades prior to being finally brought together in one ship.
4. Growing through-life technical complexity can only be delivered and sustained effectively by innovative commercial arrangements with 'rainbow teams' of large and small suppliers; these long-term relationships require two-way commitment, transparency and flexibility.

[2] EDA reporting.

5. Higher procurement costs results in fewer platforms being acquired with more integrated capability to compensate, leading to affordability and risk management issues; the vicious cycle of cost escalation, delayed delivery and reduced mass leads to indigenous industry abandoning key areas, and leaving fewer off the shelf options.

6. While significant effort is applied to delivering large-scale programmes, operational military capability is most often the result of combining those programme outputs. However there is much less focus on thematic or cross-cutting multi-platform and/or multi-domain system of systems (e.g. integrated air defence) - which will be the key enabler of future military capability.

7. Although best led by market forces, there is strategic risk in decline in the number of defence industries, as reliance on a few 'mega-primes' will create dependencies which may not be able to deliver capability and materiel scale up at times of crisis. While some may perceive it to be inefficient, industrial resilience is a core plank of national deterrence; this requires a continuous flow of expenditure on defence, albeit on occasions at low rates of production. Viable industrial independence amongst European nations – albeit interoperable with US capability and industry – incentivises cross-Alliance burden sharing; however capability programme collaboration between nations is a way to economise on effort. NATO HQ and its agencies could undertake a greater brokering role in this field.

8. Despite having academic, research and commercial industry partners participants who lead the world in the development and fielding of some of the most exciting, breakthrough technologies for a range of applications, defence innovation focuses more on 'discovering ideas' than innovation adoption. Generally high-tech, safety intensive nature requires systems thinking to be applied from the outset and early engagement of regulators.

9. Fewer forces/less combat mass than in previous eras of confrontation creates an imperative for greater interoperability and multi-domain integration. Greater rigour in enforcing common standards (STANAGs) and measuring the effectiveness of technical and procedural interoperability will be increasingly important.

10. Defence and defence industry are in competition with other (non-defence) industrial sectors for the skills required to create and sustain defence capability. An enterprise approach to the development and nurturing of relevant skills is required between public and private sectors to ensure the right number and balance exists; this will undoubtedly require closer collaboration and some employment innovation.

11. It is insufficient to focus time and resources on totemic platforms, without an equal focus on the 'dull but essential' supporting aspects such as materiel and weapons stockpiles. A revalidation of stockpile planning is required in the light of recent experience. [After note: industry should consciously work on using technology to make the operation of platforms and systems easier from both a motor skills and cognitive perspective].

Obstacles to delivery

12. Early stage opportunities to inform requirement setting and possible trade-offs, and to explore the 'art of the technically possible' are often missed due to mistrust and/or perceived compromise of competitive advantage. These obstacles can be overcome with greater openness, team working and a willingness to sanction those who breach trust.

13. Risk aversion leads to ever fewer totemic capability programmes. The resultant technical and integration risks require stringent project management controls and lead to longer procurement times and greater costs. While appropriate for complex programmes, this tends to be the pre-eminent procurement model, despite a more agile approach being suited to several needs.

14. A desire to avoid vendor lock-in and to keep commercial options open often result in through-life capability support being subordinated to gaming a competition during acquisition; this becomes a disincentive for suppliers to think long-term and invest in innovative update, upkeep and upgrade plans from the outset.

15. With a continuing platform-centric focus, defence acquisition staffs are not good at procuring and maintaining software and data management and information systems; the need to integrate and assure systems supported by AI and machine-learning will compound this problem.

16. Various nations' understandable desire to maximise the economic benefits of investment in defence and from exports of defence capability can create perverse commercial behaviours and sub-optimal capability solutions.

17. When failing to perform satisfactorily, some defence industries are not held to account; this can poison public sector thinking on closer partnering and can create perverse incentives in other industries.

Specific working group findings

18. Commercial models must be updated to reflect the need to field capability at the pace of relevance and to sustain a viable defence enterprise over time. Capability plans which 'save up' several major changes to be embodied in single programmes are both technically risky and take longer to reach the front line. While base platforms will inherently take longer to build, greater emphasis is required on their stretch potential and their various information and sub-systems to maintain an operational edge.

19. Planned and funded approaches which desynchronise the refresh rate of information and other sub-systems from their base platforms must become the norm to create the necessary agility in capability acquisition and maintenance.

20. A change to the way in which platforms are procured must be complemented by through-life 'contract for capability' approaches where multifaceted (large and SME) industry teams are incentivised to work alongside defence to invest in and embody next step improvements.

21. Greater emphasis is needed on integrating thematic multi-platform and multinational solutions – for example ground based air defence. This will underpin interoperability and multi-domain integration and ensure the right focus on data, information and software.

22. A sustainable, "independent" but interoperable European defence industrial base is both a force multiplier for NATO and will enable Europe to burden share more effectively with the US.

23. Given the premium on Western forces being able to operate seamlessly together, auditable interoperability needs to be a core part of the capability planning and industrial process, and needs to evolve through-life.

24. An enterprise approach to the development and nurturing of relevant defence technical and industrial skills is required between public and private sectors; this will undoubtedly require closer collaboration and some employment innovation.

25. NATO's national armaments directors might reasonably seek to renew the focus capability and industrial collaboration and operational interoperability by developing a defence industry 'playbook' in conjunction with its industrial advisory group for the Alliance and its closest partners.

Outlying ideas

26. Adoption of 'alliance models' which include the end user for capability development, delivery and sustainment (e.g. submarines) can greatly improve the focus on outcomes; this can also work across more than one nation (e.g. future combat air). Industrial partners can be incentivised to achieve outcomes and not solely on the judicious supply of inputs. An alliance approach can help address skills fade or lack of capacity within acquisition authorities, as it builds expertise and understanding of both user requirements and realities of the defence industrial base.

Recommended policy and the way forward

- Western investment in defence needs to increase overall – and not be managed on a stop/start basis; investment also needs to include materiel and weapons stockpiles.

- Greater emphasis is needed on integrating thematic multi-platform and multinational solutions; this will underpin interoperability and multi-domain integration, and ensure the right focus on data, information and software.

- Commercial models must be updated to reflect the need to field capability at the pace of relevance and to sustain a viable defence enterprise over time. Waiting to embody several changes in a single programme is both technically risky and take longer to reach the front line; more emphasis is required on platforms stretch potential and information and sub-systems.

- Plans and funding need to desynchronise the technology refresh rate of information and other sub-systems from their base platforms.
- Platform procurement must be complemented by through-life ‘contract for capability’ approaches where multifaceted (large and SME) industry teams are incentivised to work alongside defence to invest in and embody next step improvements.
- Adoption of ‘alliance models’ for capability development, delivery and sustainment can greatly improve the focus on outcomes, increase pace of delivery and address skills fade; this can also work across more than one nation (e.g. future combat air).
- An enterprise approach to the development and nurturing of relevant defence technical and industrial skills is required between public and private sectors; this will undoubtedly require closer collaboration and some innovation in employment and training and education.

ANNEX A

Backup notes

Desynchronised model

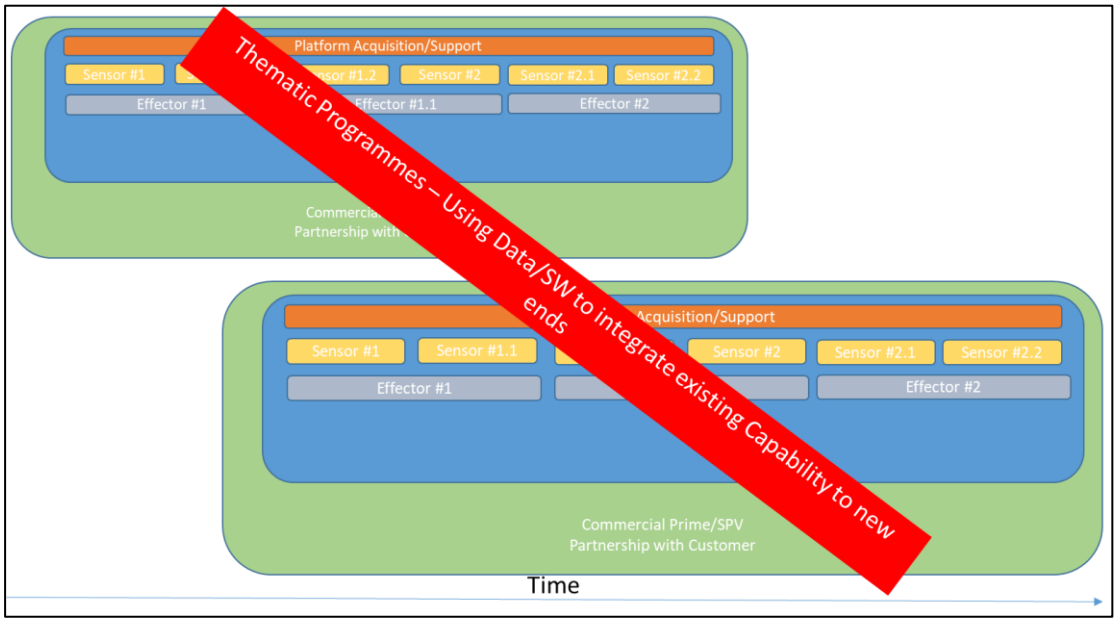

Figure 1: De-Synchronised Capability Acquisition Model

Additional notes

1. Industrial capability as part of strategic deterrence. (c.f. Cold War)
   a. Retaining sufficient 'big ticket investments' to maintain expertise, capacity and to demonstrate intent
   b. Maintenance of strong S&T investment – collaboration incentives; S&T investment is wasted if key R&D activity is not exploited quickly
   c. Persistent confrontation with adversaries and aggressors requires defence industrial base to be 'constantly ready' not just used for crisis management (e.g. Urgent Capability Requirements)
   d. Multinational effort to achieve technological superiority in key technologies
   e. Speed of moving ideas from lab to frontline is a deterrent in its own right: scale and frequency of investment
   f. Trust, transparency, long term commitment to ensure industry remains threat focused and to encourage private sector investment
   g. Keeping pace with the technology cycle: defence as first adopter or fast follower?
   h. Smart ways to be '*fitted for but not with*' capability to fit in readiness warning period
   i. Defence/nations' cultural acknowledgement of industry as 'part of the team'
   j. Defence capability used as part of nations'/NATO's readiness 'information operation'
2. National (Sovereign) vs. Multilateral.
   a. Balancing expectation of supporting own nation's export ambitions with need for international interoperability/capability commonality: bilateral/multilateral partnerships?
   b. Multinational commercial frameworks to promote international capability collaboration – enabling non-EU countries to participate
   c. 'Role specialisation' and 'lead nations' for specific capabilities: investment choices and marketplaces
   d. Approach to shared knowledge – both nationally and multinationally
3. Skills.

a. End-to-end approach on collaboration for skills between public and private sectors

b. Improve attractiveness of defence industry through *common purpose* and nature of projects and opportunities; explain/incentive with military attachments

c. Adding substance behind 'whole force' philosophy and policy: nationally/internationally

d. Accelerate cross-fertilisation between public/private sectors; use NATO to enable (and broker?) further multinational industrial cross-fertilisation

4. Resilience and security.

a. Build in resilience through-life: pre-planned upgrade/upkeep; low rate production; stockpile usage

b. Industrial capacity and supply chain audits

c. International collaboration to ameliorate supply-chain resilience: role specialisation/ lead nation. Commercial feasibility?

d. Guard against espionage on training activity disclosing capability: surrogate platforms/simulators; how to maintain physical/physiological effect of 'live'

e. Guard against industrial espionage (and sabotage); security vetting for a more fluid workforce

f. Reservists working within the Defence sector: industry risk on mobilisation

5. Agility and Innovation.

a. Disruption and competitive advantage through 'technology brokering'/bridging from civil sector

b. Proper planning for equipment/capability release with progressive assurance to accelerate programme

c. Safe spaces for testing/training in virtual and live environments (from concept phases)

d. Increase attitude to procurement risk with a bi-modal – fast-paced versus more deliberate – approach to programmes based on their type (e.g. submarine vs. UAS)

e. Taking an information-centric (information age) view to platforms; open systems as key enabler (who's open system?) for more dynamic update, upkeep and/or upgrade

f. Innovation to include creative *combinations of capabilities* and not just rapid integration or deployment of 'exotic'/exquisite technologies: measuring effectiveness

g. Risk appetite and [safe] operational use of early stage technologies: Prototype Warfare and peace time versus war approach to fielding capability

h. Coherence of innovation (nationally and internationally) and commercial innovation (and capacity) to keep pace with capability and threat need: incorporation of SMEs

i. Embedding experimentation/experimental mind-set across the capability lifecycle, rather than just an early-stage activity: means of measuring effectiveness/providing evidence

6. Operational interoperability.

a. Safe space for testing/training in virtual and live environments from concept phases

b. Rethink development and acquisition of capability away from a national platform/ system-centric model and mind-set

c. More fundamental focus [process and approach] on coherence and integration for programmatics and operations

d. Evaluation and reporting effectiveness of interoperability

e. Exploitation of simulation and other technology to improve interoperability and collective training performance without exponential cost growth.

Policy Working Group

The tasking that the Group had received was as follows: The Policy Working Group will discuss the nature of the future relationship between political authorities and military leadership – particularly in circumstances of a rapid descent into an emergency and the need for urgent decision-making in both a short-of-war crisis and war. How should this relationship be structured for optimal deterrence credibility both before and during war? Questions the working group will address will include inter alia how established rules and codes governing the conduct and restraint of warfare, including International Humanitarian Law and Rules of Engagement, might have evolved by 2035? Where will legal and ethical responsibility lie if 'learned' machines are making many decisions in the command chain? People protection will be as important as power projection in future war. What level and type of resilience will be needed of the respective home bases? It is hard to believe effective power projection can be foreseen if the home base is chronically vulnerable to information, cyber and kinetic attack? What safeguards will need to be in place to ensure democracies maintain a balance between freedom, security and privacy? How will NATO need to change? Under what rules and restraints might future war be fought, and to what ends? What level of civil defence should be aspired to and what lessons can be learnt from past practice?

The Group's discussions were focusing on two key questions:

1) How to structure the relationship between political authorities and military leadership to facilitate urgent decision-making under time pressure in both a short of war crisis and during a war and enable the military instrument of power to provide for, and contribute to, effective deterrence and defence under future (2035) political-military conditions.

2) How to maintain legal and ethical responsibility at a time, when the use of emerging and disruptive technologies, artificial intelligence and autonomous systems will significantly impact on the political and military decision-making process to compress decision-time.

Strategic environment in 2035

The Group believed that, as a first step, the key characteristics of the likely 2035 strategic environment had to be identified that would influence the political-military relationship as well as the political and military decision-making at that time significantly. To this effect, the Group established a list of key assumptions, such as:

- China and Russia will continue to be the key, authoritarian adversaries and a military challenge confronting the western democracies. The Euro-Atlantic and the Indo-Pacific region will be interlinked strategically. Adversarial developments in one region will have repercussions on the other. As a consequence, the relationship between NATO members and their Indo-Pacific partners will have become much closer than nowadays.
- There will likely be other adversaries in the Middle East/North-Africa region, such as Iran or Algeria.
- The United States will have shifted their strategic centre of gravity to the Indo-Pacific region while remaining in the Euro-Atlantic region with forces and maintaining its extended nuclear deterrence pledge.
- NATO will have implemented the Madrid Summit decisions: significantly strengthened deterrence and deterrence posture, deterrence by denial, forward defence, collective resilience, air and missile defence, adapted Defence and Investment Pledge (e.g. 2 percent/GDP for defence as a floor, not as a ceiling).
- European nations will have taken strategic responsibility and provide at least 50 percent of the forces and capabilities NATO needs. A real "burden transfer" has taken place between the US and Europe.
- The armed forces of European Allies will have been modernized, they will be capable, fully manned and equipped, trained and exercised and interoperable with U.S. forces.
- Allies will, based on lessons learned from Russia's conduct, be prepared to respond to authoritarian behaviour threatening the international rules-based order robustly and resolutely. In the run-up to a potential crisis, there is a need for determined and timely deterrence messaging, including via the considered deployment of forces.

- Emerging and disruptive technologies will have had a profound impact on security and defence and transformed the way armed forces are organized, equipped, and operate. They will have altered the character of conflict and changed the nature of war. Especially China will contest the Alliance's technological primacy. NATO's and the EU's Defence Innovation efforts, however, will have resulted in significant progress in retaining interoperability and military edge.
- Every state-on-state conflict will be of a multi-domain and hybrid nature, from information warfare to nuclear threatening, in a short-of-war crisis and in war.
- The evolution of democratic societies, the views, attitudes, and priorities of the national electorates and their security culture will still vary in 2035. A new digital generation will be focused on climate change, gender issues and continuously adapting to new technology. They will significantly influence the political-military relationship, the attitudes towards authoritarian values and behaviour, the readiness to support the use and projection of military force and accept the associated risks.
- Nations, in coordination with NATO (and the EU, where applicable) will have developed an elaborated concept of strategic communications for both contributing to deter adversaries and assuring their own populations and gaining or maintaining public support.[3]

Taking all the above parameters together, the Group concluded that future major crises and wars will have a strategic, if not global, dimension, be politically very complex and militarily very demanding. In particular, the military use of artificial intelligence, such as new generations of sensors, space-based capabilities, autonomous weapon systems, much-improved air and missile defence, drones and long-range precision missiles, by NATO/Allies and their adversaries, necessitates the ability to take urgent decisions in a crisis and immediate decisions in a war by both the political and military strategic-operational level. Precision and speed will be of the essence.

Political-military relationship

Against this background, when considering the first key question 1), i.e., structuring and developing the political-military relationship with a view to achieving the ability to take urgent decisions in a crisis and immediate decisions in war, the Group felt that in the community of democratic states key decisions would be made by key states or a group of nations, but they would at the same time seek to act through multinational institutions. The Group therefore looked at the national level (generically) as well as the multinational level, including the Alliance and partners. It concluded that building trust over time in advance of any crisis is key to cutting the decision-making process in a crisis and in a war significantly.

Measures that should be taken:

- Establish close permanent relationship and regular and frequent dialogue between the political and military leadership. The military leadership should also keep contact with the opposition party/parties as well as the party leaderships in Parliament, in order to ensure convergence of views and communicate this to the outside world.
- Set up procedures for rapid decision-making in a crisis and war in integrated rather than sequential meetings/fora at leadership level.
- Involvement of civil actors into planning of deterrence and defence, as fa as possible. Important to explore new opportunities for enhanced cooperation with key actors in civil protection and emergency preparedness. Contingency plans and the relevant cooperation between the military and the civil society must be regularly exercised as part of preparing comprehensive (total) defence.
- Exercise/conduct war-gaming based on generic scenarios for crises and war involving political, military, and civil actors.
- Transfer the above principles to the multinational and NATO level:
    - Develop structures and procedures needed to transform NATO HQ into wartime political-military headquarters at strategic level upon decision by the North Atlantic Council

[3] Comprehensive resilience is also a key requirement, but has been discussed by another Group.

    - Provide for integrated rather than sequential discussions and decision-making by the political and military-strategic leadership
    - Integrate the Supreme Allied Commander into Council discussions and decisions
    - Conduct wargaming at political level and military-strategic level based on generic, but realistic hybrid scenarios
- Continuous intelligence sharing is a must to ensure shared understanding and interpretation of data as well as joint assessment
- Euro-Atlantic governments and their Indo-Pacific partners to work on compatible strategic outlooks, develop a coordinated approach on establishing red lines and how to respond in case of adversaries crossing them. Develop structures for consultations and intelligence sharing, perhaps even decision shaping, between NATO and NATO partners in the Indo-Pacific.
- Human factor: the right people in the right place at the right time; leadership, engagement, professionalism, but also taking care for people.

Legal and ethical responsibility

As regards question 2) – maintaining legal and ethical responsibility – the Group believed there is a need for Western democracies both in the Euro-Atlantic and the Indo-Pacific region to reaffirm the value of ethical conduct in employing artificial intelligence systems on the battlefield. In other words, as a principle, there is need for maintaining an ethical approach to, and ethical standard in, operations in war and observe humanitarian law and Rules of Engagements. Any future use of autonomous systems must be based on our common democratic values and norms.

The Group believed that this requires:

- An informed debate about an appropriate approach to using AI in combat and ensuring proportionate responses
- Development of guidelines
- Preplanning, including political agreement in advance on certain situations
- Addressing ethical dilemmas that will arise, in particular in cases where an adversary ignores legal restrictions and ethical standards,
- As a preliminary guideline, differentiate between the different levels of command: At the strategic-operational level, human decision-makers should make decisions (in line with guidelines and pre-planned priorities, if possible); at tactical level, in some cases under specific circumstances, autonomous systems could decide, e.g., making choices about targets.
- There is a need for nations to follow developments in the field of AI and autonomous systems carefully, engage in the debate on their application in the years ahead and coordinate and adapt their approach continuously.

Strategy and Deterrence Working Group

Core message

The core message from the strategy and deterrence working group is that crafting a credible future deterrence strategy will require a strong but differentiated focus on the two most prominent adversaries/peer-competitors, Russia and China. Transatlantic deterrence policy will be most effective if it includes credible defence efforts by all allies in both the European and Indo-Pacific theatres in a manner that reflects appropriate capabilities and geographic location. Deterrence will have to work on the entire spectrum including nuclear, conventional, and unconventional threats. Beyond classic deterrence, the transatlantic community will increasingly have to respond to and mitigate information and cyber challenges aimed by China and Russia at destabilizing Western democracies and disrupting cooperation among them. Unless the nature of their regimes changes dramatically between now and 2035, they will likely continue to seek to rewrite the rules of the liberal international rules-based order and reshape the international system militarily, politically and economically to favour their interests and authoritarian forms of governance over those of the Western democracies.

Key Assumptions

The working group focused on NATO Allies/the transatlantic community/the West (i.e., not individual countries, and not mainly NATO as an organization

The group worked on the assumption that not all major security crises/contingencies that could affect vital transatlantic security interests between now and 2035 will necessarily be linked to a conventional, inter-state war. For example, severe collapse of states in Europe or Asia, including Russia, while posing significant challenges, would not best be managed through a deterrence lens. Prevention and pre-emption uses of power and influence might be more effective prisms through which to deal with such challenges.

So, the focus of a credible deterrence strategy by 2035 should be on how to deal with near/peer-competitors and the challenges arising from strategic competition. In this equation, China and Russia remain the main potential adversaries and sources of threats to the transatlantic community.

Working Group Findings

The risk of war between Western democracies and authoritarian states is likely to remain in 2035 or play out before that. Deterrence of threats from Russia and China will remain a key challenge to transatlantic security. The most severe threat to transatlantic security would be a full-scale war in both the Indo-Pacific & Euro-Atlantic theatres. We need to prevent this contingency and credibly signal commitment to both theatres –make sure neither China, nor Russia feel they can exploit a crisis in the other theatre. (Hold/Win & Win/Win)

We need to think not only about how to deter attacks against Allies but also about destabilizing attacks in regions of strategic importance (two—tier problem) ---investing now in boosting stability in our neighbourhood. Anchoring potentially vulnerable countries in a Euro-Atlantic framework (EU and NATO membership at the top) can contribute to a more credible defence and deterrence posture by 2035.

While both Russia and China aspire to replace the Western dominated aspects of the current international system, the threats they pose are quite different and deterrence strategies for each must be designed to be more effective for the specific threats they pose. While China is likely to become more powerful in most respects between now and 2035, Russia seems likely to become less so, except in terms of its nuclear weapons capabilities.

Transatlantic deterrence will be most effective if produced and implemented collectively. “Better together” will remain the best principle for deterrence and defence. It should operate on the entire spectrum ranging from nuclear and conventional to unconventional deterrence. Not everyone needs to do and/or be on board with everything that is required, but we need a common, integrated approach to competing and contesting.

While Allies must strengthen deterrence though their policies and actions, they should also include in their deterrence strategy approaches that weaken the will and ability of Russia and China and other authoritarian states to threaten their interests.

Effective deterrence will require raising the costs of military or political actions against Allied interests to make such actions unattractive to adversaries. This basic deterrence principle will remain central to deterrence in the near and longer term.

In a full spectrum strategic competition, deterrence alone is also not always the right prism: we need to think simultaneously about coercion, containment, deterrence and contestation.

We need to be more pro-active in shaping the international environment; simply deterring bad behaviour is not enough.

The military instrument will remain essential. Allies need to fill critical shortfalls in defence capabilities and close capability gaps. A significant U.S. commitment and presence in Europe will remain central to deterrence.

Meeting the commitments outlined in NATO's new Strategic Concept is the necessary first step. In particular, European NATO members must take more responsibility for the defence of Europe, including by recapitalizing the European defence industry. Europeans must re-learn how to manage the escalation ladder, re-think/invest in more integrated approaches to conventional-nuclear deterrence.

By 2035, European nations should be capable of providing deterrence against attacks from Russia. Eventual Ukrainian membership in NATO and the EU would enhance such deterrence. In the near term, substantial military, economic and political support for Ukraine will be essential to help Kyiv meet criteria for membership in both organizations. While NATO membership for Georgia and Moldova would not add as much to deterrence as would Ukraine's but still could add to stability.

The United States will likely continue in 2035 to play the central role in deterrence against Russian and Chinese threats to Western security and political systems.

The European and Asian allies of the United States will need to play key roles in implementing military, political, economic and financial measures in support of deterrence.

Strong and credible military instruments of power will be absolutely necessary but not sufficient for effective deterrence—diplomacy, economic tools, information operations will all need to be in the West's toolbox.

The role of resilience as deterrence by denial will gain more importance. This requires boosting societal and democratic resilience. Vulnerabilities in democratic social, economic and political systems tempt and even invite intervention by authoritarian regimes, as has been observed in the last decade.

This also requires mitigating and closing vulnerabilities to authoritarian states by reducing reliance on their energy sources and other raw materials and eliminating one-sided dependencies in trade with China.

European NATO allies, in the period between now and 2035, need to become more fully involved in deterring Chinese threats to Western security. This should include protection of key assets, technologies and infrastructure from Chinese acquisition.

NATO should expand and deepen cooperation with Asian partner states, particularly Australia, New Zealand, South Korea and Japan to enhance deterrence of Chinese and Russian challenges.

Between now and 2035, various forms of unconventional warfare, including cyber and information warfare, will increasingly threaten Western security and political stability.

Western nations will be required not only to defend their societies against such challenges but should also develop more active measures directed at Russia and China to counter and deter unconventional warfare attacks. New and innovative means must be adopted and implemented to break through the information control and misinformation on this Russian and Chinese authoritarian governance is based.

Allies should increase long term investment in science and technology programs to strengthen the foundation for deterrence in 2035.

Finally, deterrence will constantly require both European and North American Allies to improve the quality of life of their citizens and the functioning of their democracies to make them less vulnerable to the overt and covert interventions mounted by Russia and China.

Technology Working Group

The Technology Working Group divided its discussion into three broad themes: the Scope of technology; the Effects of technology; and the Management/Control of technology.

Core messages

- Technology has become another domain of conflict. Technological innovation is accelerating rapidly, changing very rapidly our expectation of warfare. And the **observe–orient–decide–act (OODA) loop** is tightening constantly. Technology is extending and altering the battlespace – it is becoming more obviously multi-/cross-domain than ever before (e.g. warfare as generalized confrontation, taking place in military, economic, social, individual spheres); it is more straightforwardly trans-regional than ever before (e.g. global reach of surveillance, targeting and strike); and it is becoming extra-regional (e.g. military competition in cyberspace, and increasing likelihood of military competition in space). Technology is also stripping away strategic depth – geography is becoming less significant in strategic planning; perhaps geography is becoming an anachronism?
- Think in terms of the action/reaction cycle and Fuller's constant tactical factor whereby **every improvement in warfare is checked by a counter-improvement, with commensurate shifts between the offensive and the defensive**. If innovation is cycling at a very rapid rate, with the possibility of decisive disadvantage for the side that reacts slowest, then there is likely to be a perceived first mover advantage. But caution: if the first mover moves too soon, too fast, then the result might not be dominance for the first mover but the beginning of an escalatory dynamic. In that case, the first mover needs to be confident that he can dominate not just a given tech sector at a given moment, but further innovation and escalation in that sector, and perhaps more broadly. (See below).

Main themes of the debate

- Scope. Emergent and disruptive technologies include: artificial intelligence, human-machine teaming, big data, drone swarms, offensive and defensive cyber, hypersonic, glide and manoeuvrable re-entry vehicles, quantum encryption/decryption, quantum precision, navigation and timing (PNT); synthetic biotechnology; directed energy weapons (DEW).
- Effect. Don't focus too closely/obsessively on a given technology. Borrowing a term from genetic research, we should consider 'recombinant innovation' – i.e. the ability not simply to acquire the technology but to mix it with other technologies to produce an unanticipated/decisive advantage. Examples: AI and autonomous platforms; AI and biotech; space, hypersonics and materials research. In these and other cases, data will be a considerably important resource – we must always be aware of the need for data assurance.
- Management & Control. Need for a dynamic, adaptive 'mixing mind-set' with emphasis on speed if we're to maintain cognitive confidence and dominance. Our ability to combine technologies should be considered a constant, rather than a singular end-state.

Obstacles to delivery

- Acquisition/procurement processes that discourage continuous, adaptive innovation and (financial) risk once project is confirmed. Too often this approach to acquisition has produced gold-plated, unusable, vulnerable products – and too often far too late.
- Interoperability. Not a new topic – NATO has been addressing this since the 1950s. But the growing gulf between technologically advanced allies and 'the rest' can create problems for interoperability and force cohesion. So, while we might prefer/have as our goal perfect, 100% interoperability, we have to be pragmatic and, in certain circumstances/with certain allies, accept coherence as the next best thing.
- If technologically advanced allies develop **Concept of Operations (CONOPs)** that the less technologically advanced allies cannot follow, then we have a problem. So, wherever possible, we should develop both CONOPs and technology together and then exercise them together. When we can't do so, then we need to consider appropriate (and agreed) divisions of labour – e.g. with BMD.

- Paradoxically, greater interoperability can create vulnerabilities – particularly when different levels and types of technology are not fully de-conflicted.

Specific Working Group findings

- Deterrence has eroded and we need to develop visible, costly signals to impress upon adversaries not to act. We need to be seen to be remedying problems and gaps: we can't play catch-up with our deterrence posture/messaging – we must be seen to be adapting 'at the pace of relevance' (**Jim Mattis**). It's relatively easy to measure the erosion or failure of deterrence, but we need also to measure (or at least argue for?) its effectiveness. In some cases a strategy of ambiguity can have deterrent effect. But in other cases, it might be clarity that is more convincing.
- Possibilities of increasingly sophisticated (and credible) deep fake technology has implications for cognitive confidence.
- First mover might gain the advantage but this brings with it escalatory risks.
- Expanded domains need to be integrated into current processes that themselves will require adaptation.
- Consider division of labour within the alliance in tech development and application.
- Does the Alliance need a 'Project Air Force'/RAND approach for the 21st century?

Outlying ideas

- We should also not overlook the fact that in some cases, high levels of technology (or, at least, highly decisive levels of technology) can have relatively low barriers to entry. Some cheap and adaptable technology (e.g. drones) could confer decisive advantage on small state and non-state actors.
- OODA loop. Tightening cycle of innovation using AI and quantum raises spectre of 'crowding out' the human. This is orthodox analysis. But can we see it differently? Perhaps tightening of the 'OOD' will have a 'crowding out effect, but if the human can remain in or on top of the 'A' then this could be an optimal outcome. Fidelity of information and intelligence is improving fast, thanks to technology – we have greater understanding of 'what' is happening. But 'why' it is happening remains difficult – beyond machine judgement and still the domain of the human brain.

Recommended policy and the way forward

- Strategic discipline needed over tech investments that by necessity must increasingly be public-private partnerships. We need to discriminate, prioritise and select. We're familiar enough with evolutionary innovation, but we also need to sensitise ourselves to the possibility and effect of revolutionary innovation – the 'paradigm changing' disruptions.
- Should we continue to teach mission command? Yes. Our preference and our greatest strategic asset is a distributed **Command and Control (C2)** structure. This makes mission command essential. But we must mean it! We mustn't just teach the theory of **Military Command (MC)** to young officers and NCOs, we must trust them in the way that MC requires – trust them when they succeed and, critically, when they fail. Anything else is centralized C2 by another name.
- More work required on the ethical and legal dimension of technology. We're working in an ethical framework that is way behind the science. The ethical framework for technological innovation is missing.
- More use of simulations and crisis management scenarios for policy planning and decision-making and involve more scientists in these.
- On the (tired?) topic of the relationship between platforms and systems. The platform/systems balance is always in flux. Platforms are still relevant, of course. But perhaps they're more obviously significant in peacetime, when they can serve as an expression of intent. But in time of conflict, its systems, and the integration of defence capability that produces potency and decisive capability. This takes us back to the theme of agility and adaptability. Just as we need 'recombinant innovation', so we need rapid re-configurability 'at the pace of relevance' (not a decade later, when things have moved on).

- Whatever the combination of platforms and systems, we should also bear in mind that complexity not only offers resilience, it can also (if not monitored very closely) create dependence. And unmitigated dependence creates vulnerability.
- What can we expect from arms control and similar, treaty or MoU-based approaches to stabilizing tension? Can we negotiate restrictions on AI, quantum, and biotechnology as well as dis/misinformation and deep fakes analogous to the conventions on biological and chemical weapons? Or should we settle for something more modest at this stage – perhaps basic risk reduction measure and the Confidence Building Measures that emerged in the early years of the Cold War?
- As well as high-speed, we will need high lethality. This accentuates the difficulty in cultivating public support for the use of armed force. But also the necessity to do so. In democracies, armies, navies and air forces fight wars, but its countries that go to war. In this regard, we need to improve security & defence outreach and education.