



Ministry
of Defence

Future Operating Environments 2040

Future Operating Environments 2040

March 2026

Assistant Chief of the Defence Staff
(Futures and Force Design)

Conditions of release

This publication is UK Ministry of Defence (MOD) Crown copyright. Material and information contained in this publication may be reproduced, stored in a retrieval system and transmitted for UK government and MOD use only, except where authority for use by other organisations or individuals has been authorised by a Patent Officer of the Defence Intellectual Property Rights.

The content of this publication does not represent official policy or strategy of the UK government or that of the MOD.

Authorisation

Defence Futures is responsible for publishing strategic trends and concepts. If you wish to quote our publications as reference material in other work, you should confirm with our editors whether the particular publication and amendment state remains authoritative. We welcome your comments on factual accuracy or amendment proposals.

Email: MSHQ-FFD-Digital@mod.gov.uk

Copyright

This publication is UK Ministry of Defence © Crown copyright (2026) including all images (unless otherwise stated).

If contacting Defence Intellectual Property Rights for authority to release outside of the UK government and MOD, the Patent Officer should be informed of any third party copyright within the publication.

Crown copyright and Merchandise Licensing, Defence Intellectual Property Rights, Central Legal Services, MOD Abbey Wood South, Poplar 2 #2214, Bristol, BS34 8JH. Email: DIPR-CC@mod.gov.uk

Distribution

Our publications are available internally to MOD staff from the Leidos Forms and Publications Team using the Millie Online Portal.

Email: leidos-formspublications@teamleidos.mod.uk

Digital versions of our publications can be viewed and downloaded on defnet at: <https://modgovuk.sharepoint.com/sites/IntranetCSOC/SitePages/defence-futures.aspx>

This publication is also available at: <https://www.gov.uk/government/groups/defence-futures-and-force-design-ffd>



Foreword

The *Strategic Defence Review 2025* (SDR 25) reminds us that the security environment is unpredictable: ‘the UK faces multiple, direct threats to its security, prosperity, and democratic values. The world itself is beset by volatility and deep uncertainty.’ Moreover, as *Global Strategic Trends: Out to 2055* (GST 7) highlights, the forces shaping the coming decades will be contradictory in both time and place. Yet there is still significant value and importance in understanding how the future could plausibly transpire and, more specifically for the defence sector, understanding the sort of future environments in which the UK military might have to operate and fight. This is what *Future Operating Environments 2040* seeks to do, building on the foundations of GST 7.

Furthermore, publishing this work supports informed dialogue and broad engagement across government, industry, academia and wider society. Its release is also intended to deepen collaboration and encourage a whole-of-society approach to strategic preparedness, another clear theme of SDR 25. As the operating environments of tomorrow will be defined by continual change and complexity – conditions no single actor can navigate alone – placing this assessment in the public domain invites partners to examine, challenge and contribute to our evolving understanding. It deliberately explores multiple potential environments in the future and is offered not as a definitive forecast, nor a statement of intent, but as a shared foundation for planning and resilience in an increasingly interconnected world.

Air Vice-Marshal Mark Ridgway DBA
Assistant Chief of the Defence Staff, Futures and Force Design

Contents

- Foreword 3
- Introduction. 7
 - Purpose 7
 - Structure and navigation 7
 - Method and framework 8
- Part 1 – Future Operating Environments 2040 11
 - Section 1 – Drivers 11
 - Section 2 – Actors 13
 - Section 3 – Relationships 17
 - Section 4 – Characteristics. 18
 - Section 5 – Spaces 20
 - Section 6 – Technology convergence 25
- Part 2 – Disruptors 29
 - Section 1 – A snapshot of threat multipliers 29
 - Section 2 – A snapshot of novel and disruptive capabilities . . . 32
- Key takeaways 37
 - Good bets 37
 - Probable bets 40
 - ‘High impact, low probability’ bets 40
- Glossary 41
- Acknowledgements. 43

Introduction

Purpose

A complex set of global dynamics that influence, counteract or accelerate each other is rapidly changing the global security environment. *Future Operating Environments 2040* (FOEs 2040) aims to describe these likely characteristics and dynamics. Pinpointing when specific change will emerge in any long-term assessment is, however, invariably problematic. To that end, the purpose of this publication is to offer an overview of tomorrow's operational and operating engagement spaces and, in addition, offer insights into alternative plausible outcomes.

It is designed primarily to provide evidence-led insights to inform UK Defence's policy and strategy direction, future force design and capability strategy. FOEs 2040 is also intended to be useful for Defence's partners – including across the UK government, the North Atlantic Treaty Organization, academia and industry. More broadly, it forms part of the Military Strategic Headquarters' Futures and Force Design conceptual thinking and, as such, it can be used to test assumptions for future force development and force blueprints beyond planned force testing cycles.

Structure and navigation

FOEs 2040 is organised into two primary sections with the key takeaways presented at the end of the publication. These are outlined below.

- a. **Part 1 – Future Operating Environments 2040.** Part 1 focuses on the key factors and actors that will shape the future operating environments and explores their geographical and contextual settings.
- b. **Part 2 – Disruptors.** Part 2 examines the disruptors that are expected to transform the conduct of operations. The analysis is split into threat multipliers and novel and disruptive capabilities.
- c. **Key takeaways.** The key takeaways are summarised as either 'good', 'probable' or 'high impact, low probability'. These 'bets' reflect the three lenses applied during our analysis.

- (1) **Good bets.** Good bets are characteristics that appear consistently across all the different futures examined. Their recurrence suggests that these are reliable areas for future force design to address directly.
- (2) **Probable bets.** Probable bets are characteristics that appear in many of the futures, being noticeably prevalent and impactful. These are areas that force designers would be prudent to address, given their likelihood and significance.
- (3) **‘High impact, low probability’ bets.** These are characteristics that are considered unlikely to occur but, if they do, would have profound and far-reaching consequences. For these, it is sensible to either develop contingency plans or consciously accept the risk of not doing so.

Method and framework

At the core of FOEs 2040 analysis is an extensive horizon scan of the strategic landscape for emerging trends, threats and opportunities that may shape future operational contexts. The analytical and research process included a series of internal and external workshops involving a range of stakeholders and experts – from Defence, as well as science and technology organisations. Collaboration with global partners also provided a broader view and diverse insights. Further detail is included in the acknowledgements section at the end of the publication.

The FOEs 2040 deliberately adopts a pluralistic approach, reflected in its title. This is a recognition that the security environment is increasingly unpredictable, characterised by continual change, contradictions and inconsistencies. Selecting a singular view of the future operating environment in 2040 is therefore insufficient to capture the inherent complexity and dynamism.

This assessment is the result of an intensive and rigorous process that tested the defence implications across five distinct illustrative pathways towards the future world order. These pathways represent a spectrum of plausible global developments, encompassing varying geopolitical alignments, technological advancements and societal shifts. The final analysis presented in FOEs 2040 captures the core commonalities that emerged across all five future worlds in *Global Strategic Trends: Out to 2055*.

FOEs 2040 does not aim to provide an exhaustive assessment of all potential scenarios, actors or technologies. Instead, it focuses on summarising principal factors in a manner that is accessible and easy to understand.



Part 1

Future Operating Environments 2040

Section 1 – Drivers

Six global interacting drivers of change will shape the long-term future. These drivers will influence, counteract or accelerate each other in complex and often unexpected and contradictory ways. They will vary across regions, and be influenced by the choices various actors make, but will also combine to form the future security environment in which the future operating environments (FOEs) exist.

Global power competition. Competition and strategic rivalry will continue, with states likely to remain the principal actors. Major powers will remain prominent but face increasing challenge from regional and non-state actors interacting in dynamic ways for their own advantage. These developments could destabilise the previously established international order and heighten risks of miscalculation, particularly in contested spaces. Shifting dynamics will, in part, determine whether the FOEs exist within frameworks bound by multilateral rules and norms, or a more fragmented and polarised global order.

Demographic pressure. The global population will continue to grow and age unevenly, albeit with significant regional variations. Urbanisation will rise with many cities becoming increasingly technologically assisted and data driven. This will be as much in response to a declining and ageing workforce as to gain strategic advantage. Demographic changes could result in an operating environment that is aggravated by worsening inequalities, political unrest, large-scale migration and intensive competition for resources.

Climate change and pressure on the environment. An increasingly chaotic climate will transform geography, economies, societies and power structures as irreversible change drives migration and resource insecurity. Resource ownership, access and access rights will continue to shape the geopolitical landscape, in new regions and locations as well as existing ones. The FOEs will be characterised by a degraded and changing physical environment where defence organisations may increasingly need to assist in managing

climate-related risks. Planning assumptions, logistics, training, access and capability operating envelopes will need to be reviewed and possibly revised.

Technological advances and connectivity. Technological advancements and the proliferation of hyperconnected data are poised to redefine military capabilities and the very character of warfare. These developments will influence the speed and direction of change across all drivers of change. The FOEs will see significant investment in technological innovation as both developed states and non-state actors strive to seek advantage. Sole reliance on high-end capabilities and technological advances, however, cannot guarantee success where the interplay between strategy, intellectual capital and technology development will be key. The FOEs will therefore be simultaneously asymmetric and high-end, where actors will integrate new technologies with current capabilities in pursuit of operational advantage.

Economic transformation and energy transition. Beyond economic and energy frictions as a cause of conflict, defence and security may need to adapt to disruptions in global supply chains and the operational implications of the energy transition. Perceptions of equitable access to essential resources and technology, and how actors choose to cooperate (or not), will exacerbate tensions. Defence actors that are tightly coupled to fossil fuel energy sources will become increasingly vulnerable to supply disruptions. The FOEs will likely see shifts in global markets, supply and value chains, and a changing notion of globalisation. There is also likely to be a mismatch as security actors seize opportunities to transition to new fuels as well as exploit the advantages of automation.



Cities of contrast: inequality fuelling instability in an interconnected world

© AsiaTravel / Shutterstock.com

Inequality and pressure on governance. Further advances in connectivity will continue to feed increasing real or perceived inequalities and fuel tensions that could be exploited. Increased urbanisation means this will occur in more complex physical and human terrain. Independent or collaborative defence and security activities will be challenged consequently, especially in resource-scarce locations where they worsen life for the host population, even if only temporarily. Risks resulting from inequality and pressure on governance mean the FOEs will be complex and unpredictable, with levels of societal resilience key to stability and advantage. Supporting governance reforms and fostering sufficient international cooperation to address the root causes of instability may become essential to mitigating the security implications of such inequality and weak governance.

Section 2 – Actors

The number and diversity of security actors will increase significantly by 2040, with a growing presence of non-state entities engaging in military and security activities. States will likely remain principal interlocutors, however, the number and type of security actors will rise. Although the United States (US) and China are likely to remain highly influential, both face considerable domestic challenges, which may disrupt their standing. The long-term role and influence of Russia remains uncertain; India and the European Union (EU) have considerable shaping and network-building potential. Today's middle powers are likely to retain a certain degree of influence. Emerging powers, new blocs of states and non-state actor networks may expand their outreach, and their strategic choices may influence the global power balance in unexpected ways. These developments may see the continued diffusion of global power beyond major state actors, and possibly a blurring of the boundaries between state and non-state actors. States, proxies, serious and organised crime groups, violent extremist organisations, and private military contractors will vie for space and influence, resulting in a congested operating environment that is difficult to coordinate, command and control.

United States of America. The US will continue to assert substantial influence across all levers of national power, although the country's role as a global actor will be less predictable. Their ability to balance foreign and domestic public opinion during times of global tension will remain a challenge. Defence resources are likely to further reorientate from the Euro-Atlantic to Indo-Pacific

regions, the Western Hemisphere and the First Island Chain.¹ Although the US will continue to operate in cooperation with allies globally, there will be shifts in burden-sharing standards with US forces and industrial base increasingly focused on mainland defence.

China. China will retain a long-term outlook focused on protecting its core security interests by strengthening military forces (including nuclear), economic reach and diplomatic efforts both regionally and globally. China will continue seeking strategic advantage through extensive espionage, cyberattacks, and the acquisition of cutting-edge intellectual property by both legitimate and illegitimate means. Its rapid and large-scale military modernisation programme will be marked by substantial increases in advanced platforms and space warfare capabilities, as well as the diversification and growth of its conventional and nuclear missile forces, many of which could reach Europe. Its stance on Taiwan is unlikely to change. An expansion of deployed military capability to safeguard economic investments and trade routes is anticipated.

Russia. Russia's aspiration to retain its great power status, or reclaim that of the Soviet Union, may be sought at the expense of domestic development. It will likely remain focused on hard competition over indirect influence and resources. Wartime overstretch could significantly impact an already economically stagnant Russia and see it have increasing dependence on China, as well as other trading partners such as India and Iran. It is possible that Russia may increasingly be seen as part of the Chinese sphere of influence.

India. Should India shift its non-alignment position, it has potential to exert significant influence in the global political order. Its large population, geographic position, relationship with the US, China and Russia means that it could have a significant global shaping role.

Middle and emerging powers. Developed countries with advanced economies, such as the Group of Seven (G7),² will retain substantial global outreach, leveraging alliances, multilateral and minilateral organisational memberships and diplomacy. Several emerging powers, especially Emerging Seven (E7)³ countries are likely to become key players. Their rise may lead to the creation of new and influential geopolitical blocs or the disruption of existing ones.

1 The First Island Chain is the first string of major Pacific archipelagos out from the East Asian continental mainland coast.

2 The G7 is an intergovernmental political and economic forum comprising Canada, France, Germany, Italy, Japan, UK, US and the EU as a 'non-enumerated member'.

3 Brazil, China, India, Indonesia, Mexico, Russia and Turkey.

Multinational and conglomerate corporations. Multinational corporations, whose turnovers exceed those of many countries, already dominate many areas of technology and intellectual property. Rising costs and supply chain complexities may further concentrate power amongst a few high-value companies, creating monopolies through research aggregation and aggressive acquisition of emerging technologies. States dependent on these monopolies risk losing competitive advantage and data security confidence. Outsourcing to commercial actors compromises state control, while wealthier entities may bypass state-led capabilities by purchasing military power. Pay-to-play models could destabilise international security through their withdrawal, conditional services or misuse of capabilities.

Super-empowered individuals. Super-empowered individuals, such as super-wealthy business and religious leaders, and other influential figures, will play a greater role in shaping power dynamics, acting as disruptors, motivators, mediators and peacemakers. The influence of these individuals is expected to expand, potentially rivalling that of some states.



Axis of influence: strengthening ties in defiance of global norms

Cities and sub-national entities. The continued rise of megacities through urbanisation and economic concentration may see them surpassing states as hubs for development and influence. Their narrower focus of governance, compared with states, could permit them to act in ways perceived as more responsive to the needs of their citizens. Differences in innovation and wealth could lead to cities or autonomous regions influencing their parent states or even seceding, particularly in areas with strong political or ideological views. Advanced cities or areas within less-developed states may even dominate, inverting the traditional governance relationship. It is plausible that such cities may hold militaries or military powers in their own right.

International and regional organisations and partnerships. An escalation in global power competition will have an impact on the institutions that make up the international system. Regional blocs and alliances, including military ones such as the North Atlantic Treaty Organization (NATO), will most likely see similar patterns to those of global institutions, linked to their ability to deal with multiple destabilising factors, shifting priorities and agendas within and between member states. Digitally based alliances or interest organisations that include powerful non-state actors could become even more influential than traditionally geographically based ones.

Non-governmental organisations and charities. Third sector actors – including non-governmental organisations, advocacy groups and other civil society organisations – are likely to expand their outreach and involvement within conflict spaces. Some will remain impartial, while others may act in accordance with their own values or on behalf of other actors, sometimes with hostility. This will affect freedom of movement dynamics and action for defence and security.

Violent extremist organisations and criminal actors. Armed political and ideological factions will gain sophistication and acquire access to even more capabilities that were previously restricted to states. Their control of territory also provides havens for other malign actors or activities, and their willingness to exploit contested and ungoverned spaces could create or exacerbate existing political, identity or ideological tensions. The line between state and non-state authority is expected to blur further, reinforcing a world where security, stability and influence are perpetually negotiated among a diverse range of actors.

Proxies. The deliberate use of willing and unwitting proxies – and increasingly ‘clients’ – will continue, enabling activities deemed too sensitive for states or where an alternative messenger is beneficial. Examples include state initiatives,

such as China's Belt and Road Initiative to enhance geopolitical influence through third parties, while other powers like India may use digital services for similar purposes. Multinational corporations will also be involved both as proxies and agents in this struggle for influence. The ability to disguise or reveal the consequences will be a focus in the information environment. Employing aid to gain support and influence in multinational fora will also continue, whether based on altruism, conflict avoidance or for purely transactional benefit.

Countries at risk of instability. Countries at risk of instability will face layered drivers of fragility, creating compound effects that may threaten even those that appear stable. The relative strategic advantage of individual states within alliances and coalitions will be accompanied by varying degrees of trade-off concerning the success, failure, agenda and approaches of others. Overlapping bilateral, minilateral and multilateral security arrangements are likely as actors seek more beneficial or aligned outcomes.

Section 3 – Relationships

The balance between global cooperation and fragmentation in security approaches will fundamentally shape the FOEs. Expanded and extended arrangements of existing alliances could form in response to shared threats. Pressing existential challenges may drive global actors towards fundamentally cooperative approaches, where aligned security interests reduce the risks of conflict. Conversely, in a more fragmented scenario, states may align with like-minded peers or resort to unilateral defence and protectionism, competing aggressively with others.

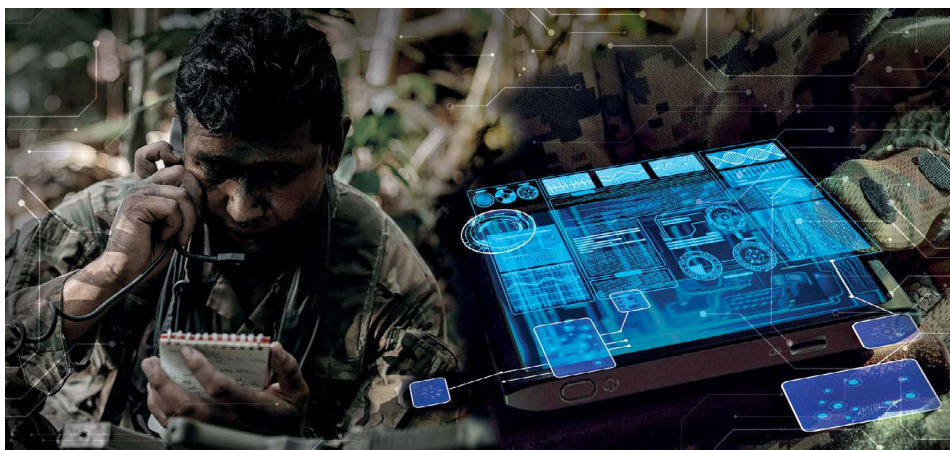
Existing adversarial relationships between major, emerging and middle powers are likely to endure, but may fluctuate between indifference, obstruction, hostility, tolerance and issue-based cooperation. Border disputes, sovereign claims to territory and resources, and internal disputes over the distribution of power and wealth will persist, especially those tied to historical tensions around identity, religion, ethnicity and nationalism. Flashpoints may remain localised or spill over with regional or even global impacts, depending on the actions and inactions of actors within wider ecosystems. A violent, drawn-out conflict in the Euro-Atlantic or Indo-Pacific regions, involving the NATO Alliance, could frame the wider context of tomorrow's operating environment.

Future strategic partnerships are likely to be more pragmatic and less dependent on shared values and ideals. Major powers may become increasingly selective in their engagement. More broadly there may be an increasing trend towards 'withdrawalism' from treaties and resistance to the meaningful reform some actors wish to see. Emerging powers, new blocs of states and non-state actor networks may expand their outreach, and their strategic choices could influence the global power balance in unexpected ways. States may increasingly reject multilateral treaties and other legally binding agreements in favour of informal non-binding single-issue arrangements, giving rise to a proliferation of minilateral or bilateral issue-centric coalitions. It is possible that the current system could collapse. Alternatively, the impact of creeping polycrises could lead to a fundamentally new kind of multilateralism. There is a clear trend towards power diffusion and a more crowded stage, requiring Defence to be agile in forming and adapting partnerships to maintain strategic advantage.

Section 4 – Characteristics

The FOEs of 2040 will be both revolutionary and evolutionary. Rapid and radical technological change will coexist with the continued relevance of less sophisticated and/or legacy systems. The operating environment will be simultaneously asymmetric and high-end: small states and weaker actors may prevail over major powers by leveraging whole-of-society efforts and unconventional tactics. Defence actors, regardless of size, will pragmatically combine new technologies with existing capabilities to gain operational advantage. Sole reliance on advanced capabilities will not guarantee advantage, especially if access to the critical operational domains of space, and cyber and electromagnetic is denied. In such scenarios, actors may revert to using obsolete or abandoned systems, which could provide unexpected resilience and redundancy. The retention and adaptation of legacy capabilities may therefore remain a source of advantage.

The characteristics of FOEs will fundamentally stretch the concept of homeland defence beyond traditional physical and geographical boundaries. Defence will be required not only to protect territory and critical infrastructure, but also to safeguard national interests and ensure freedom of manoeuvre in cyberspace, space and the information environment. The boundaries between homeland and external operations will become increasingly blurred, as will the distinction between competition, crisis and conflict. This growing ambiguity will demand greater civil-military cooperation, mobilisation and integration, with a whole-of-society approach becoming essential for effective defence in an environment marked by strategic uncertainty.



Navigating the complexities of 2040 warfare: blending legacy systems with cutting-edge technology

The proliferation of data, the rise of sophisticated computing capabilities and the interconnectedness of systems – combined with rapid technological advancement – will extend and merge operational domains. It will be hard to maintain technological superiority. Future warfare will span from subsea and deep sea to subterranean and deep space, traverse the electromagnetic spectrum, and permeate augmented, virtual and cognitive spaces. These features will form the backdrop against which actors compete for advantage, often simultaneously across multiple operational domains and spaces.

In practical operational terms, the FOEs of 2040 are likely to be characterised by hyper-dispersed forces operating across large geographic areas while remaining digitally interconnected. Units may rely on artificial intelligence (AI)-enabled mission command to operate semi- or fully independently when communications are degraded, requiring a shift from platform-centric to resilience-centric approaches. The density of machine-generated data, alongside the speed of future operations, will demand new cognitive skills and augmented decision support to prevent overload.

Evolution in conventional warfare will eventually see greater attention on gaining and maintaining advantage through resilience, adaptability and distribution of assets. This may result in diverse, resilient or even redundant forces, which runs contrary to some interpretations of efficiency. These broader environmental characteristics could lead to flexible and adaptive approaches being adopted across the full spectrum of activities, including those below the threshold of armed conflict. It could also mean greater levels of integration are sought for operational advantage (between Services, across government and society, and between human and machine-enabled capabilities).

Traditional concepts of deterrence by denial or punishment will remain relevant, but the means of achieving them will evolve. However, other models⁴ might be explored by other actors. Understanding why a model is selected may offer useful insight. Forging alliances for extended deterrence (security guarantees provided by nuclear weapons states) might become important for some non-nuclear nations. Nuclear deterrence will remain the shaper of strategic stability between nuclear weapons states. The balance of assured second and third strike, mutual vulnerability and credible retaliation will endure but strategic stability will face new challenges.

Section 5 – Spaces

Maritime

The maritime operating environment will become increasingly accessible and reachable, driven by continued advances in maritime technology. These technological developments are expected to unlock the maritime environment for a wider range of actors and a broader array of uses. Climate-driven changes, such as the melting of polar ice, may open new sea routes, transforming previously inaccessible areas into contested spaces and increasing the demand for maritime presence and security.

The expansion of emergent and future infrastructures, along with growing commercial interests at sea, will introduce new security tasks and dilemmas for Defence. The proliferation of monitoring and sensing technologies will make the world's seas more visible and transparent than ever before, reducing the ability to operate undetected and increasing the complexity of maritime operations. At the same time, advances in hypersonic cruise missiles and supercavitating torpedoes will extend the range and lethality of threats, heightening risks to naval and commercial vessels alike.

Maintaining freedom of manoeuvre and ensuring maritime security will become increasingly challenging for Defence. The heightened visibility of maritime spaces could lead to new approaches to concealment, deception and operations security, while the proliferation of advanced weapon systems will require further investment in enhanced defensive measures and rapid adaptation to emerging threats.

.....
⁴ Deterrence by entanglement creates inter- and cross-dependencies and linkages between countries, alliances and amongst adversaries to introduce mutual vulnerability and therefore deter aggression. Deterrence by variety is a strategy involving the maintenance of highly resilient but also redundant capabilities and assets to maximise the cost of attacks and minimise impact.

Land

Land operations will take place in environments that are increasingly cluttered, digitally connected and exposed. The future land engagement space will encompass a diverse mix of smart cities, affluent and impoverished areas, industrial complexes, poorly or superficially planned zones, and informal or slum dwellings – often within the same area of engagement. This complex urban landscape will drive both restraint and the need to adapt tactics for operating in densely populated settings.

The presence of large populations in both high- and low-technology cities will make these urban centres persistent targets for adversaries. The interconnectedness of urban infrastructure and the proliferation of digital technologies will further complicate efforts to isolate or control these spaces. In such digitally enabled environments, adaptation and masking will become increasingly difficult, as advanced surveillance and data-driven systems reduce opportunities for concealment and manoeuvre.

These trends mean that land operations will require new approaches to adaptation, deception and survivability in technologically assisted and data-rich environments. The FOEs are likely to feature novel capabilities, operations in more congested or opaque settings, and a greater reliance on subterranean spaces for movement and protection. Successfully operating in this environment will demand agility, innovation and the ability to integrate both advanced and traditional tactics to maintain operational advantage.

Air

Air operations will be significantly expanded, evolved and increasingly complex due to the democratisation of technology, the proliferation of dual-use equipment and the growth of the global aerospace market. A wider range of actors – including those previously lacking advanced capabilities – will gain access to combinations of mass and innovation, enabling even unlikely adversaries to create lethal effects in the air domain.

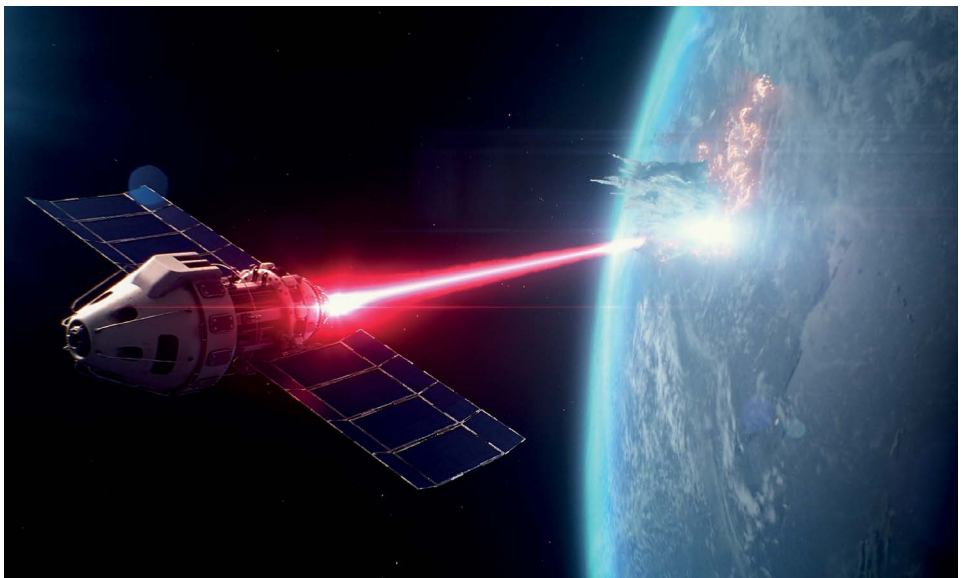
The deliberate congestion of airspace, both before and during armed conflict, will become a common tactic to restrict freedom of action and complicate operations. In this environment, the speed at which new air capabilities can be fielded and adapted will be critical in determining which assets remain credible, resilient and relevant.

The intentional crowding of airspace will demand new approaches to airspace management, deconfliction and operational planning. The continued proliferation of hypersonic glide weapons and drone swarms will increase the threat to both military and civilian infrastructure, requiring enhanced defensive measures and rapid innovation in countermeasures. Maintaining air superiority and operational effectiveness will depend on agility, technological adaptation and the ability to respond to a rapidly evolving threat landscape.

Space

Space will play an increasingly central role in societal, economic, defence and security activities, making it of growing strategic importance. As a result, space could become both militarised and potentially weaponised. While the prospect of general space warfare remains uncertain, the development and deployment of lunar-based or co-orbital missile defence systems is more than plausible, signalling a shift towards the weaponisation of space assets.

The entanglement of military and civil space infrastructure will make it increasingly difficult to distinguish between peaceful and military uses, whether these are overt or covert. Multiple actors – state and non-state alike – will compete for capacity and positional advantage across all orbits, driving the need for more rapid deployment, reconfiguration, protection and defence of space assets.



Orbital dominance: precision strikes from the final frontier

© Frame Stock Footage / Shutterstock.com

Existing civil and military satellites could be repurposed or weaponised, blurring the lines between civilian and military targets and complicating efforts to ensure the security of space-based capabilities. At the same time, the emergence of new satellite constellations may provide resilient, adaptive and low-latency communications, even in significantly degraded environments.

Cyber and electromagnetic

Cyberspace and the electromagnetic spectrum will remain critical for both military and civilian activities. Advanced cyber technologies will enable actors to create significant effects with relatively few deployed personnel, expanding the scope and reach of global campaigns. As accessibility and connectivity increase, so too will the number of potential attack surfaces, making networks and systems more vulnerable to intrusion and exploitation.

Spectrum denial and manipulation are expected to become more prevalent during military operations, as sophisticated adversaries seek to disrupt, degrade or deny connectivity to undermine network-dependent effects. Data-centric warfare will be common, with adversaries aiming to access, poison, mislead or deny the use of critical data. This environment will drive a growing demand for alternative and resilient services that are less reliant on cyberspace or the electromagnetic spectrum. Some actors may pursue complete data and cyber sovereignty, further complicating the operational landscape.

Hyperconnectivity will enable increasingly sophisticated information activities, allowing adversaries to target individuals, groups or organisations, and threaten critical functions, such as finance, health care and the security of personal data. As quantum technology matures, it will introduce entirely new magnitudes of challenge, potentially rendering current encryption and security measures obsolete and fundamentally altering the nature of cyber and electromagnetic operations.

Subterranean

Driven in part by advances in sensor technology and an increase in long-range capabilities, it is likely the subterranean environment will increase in importance. It could support operational continuity in high-intensity conflicts through hardened hubs and facilities. Industrial digging and mining expertise could expand the use of the subterranean environment at scale beyond urban developed locations. Subterranean locations could provide resilience

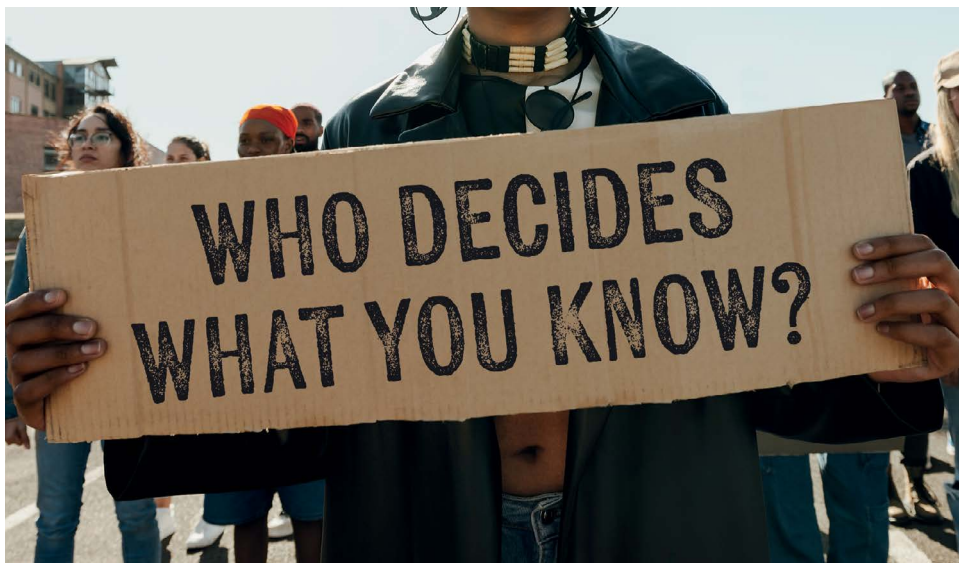
of civil and specialised infrastructure. The development of counter-capabilities is expected to drive advancements in technologies such as seismic and electromagnetic sensing.

Cognitive

Cognitive effects will remain central to shaping the perceptions and behaviours of both decision-makers and broader populations. However, the cognitive operating space will become increasingly blurred and potentially untrustworthy. The proliferation of information and data, combined with the influence of social media algorithms, deep-fake technologies and widespread misinformation or disinformation, will amplify both accidental and deliberate narratives.

In this space, adversaries will be able to manipulate information to influence public opinion, decision-making processes and societal cohesion. The sheer volume and velocity of information will make it difficult to distinguish between truth and falsehood, increasing the risk of confusion, mistrust and polarisation.

Deliberate targeting of populations and institutions through information operations could erode societal norms and weaken trust in authorities. This could undermine long-term defence readiness and industrial resilience. It may also alter how populations respond to the behaviours of other actors as well as their own approach to constraint and restraint.



Cognitive warfare: shaping perceptions, eroding trust and engineering truth

Adapted from © Jacob Lund / Shutterstock.com

Law

The FOEs are likely to be shaped by the strategic manipulation of legal frameworks, as adversaries exploit international law and areas of legal ambiguity to advance their objectives. The evolving legal landscape will see both state and non-state actors leveraging legal mechanisms to challenge sovereignty, disrupt military operations and influence global norms. Adversaries are expected to employ 'lawfare' tactics, such as selective treaty interpretation, exploiting ambiguities in customary international law or creating regulatory uncertainty to constrain state actions while remaining technically within the bounds of legality.

Out to 2040, the proliferation of data will increasingly strain institutional processes, as the sheer volume of evidence risks overwhelming mechanisms for timely legal rulings. Emerging technologies (including autonomous systems, AI and advanced cyber capabilities) will introduce novel legal challenges, such as issues of accountability, attribution and compliance with international humanitarian law. Non-state actors are also expected to play an increasingly significant role, using legal tools to influence state behaviour, challenge regulatory frameworks and shape public opinion. The legal domain will no longer serve merely as a backdrop to conflict but will evolve into a dynamic and contested operating space. Success in this operating space will require the ability to anticipate, navigate and shape legal developments, making legal acumen as critical as traditional military capabilities.

Section 6 – Technology convergence

The compound effects of technology will drive evolutionary changes in military operations and campaigns. Their impact will vary according to the level of sophistication, practicality of fielding and the aspiration of the user. Consequences for decision-making, information processing, delivery and targeting, and attribution will remain key variables in warfare and deterrence. However, advanced and exquisite technologies may be countered by massed, inexpensive and often commercially available solutions. Importantly this will likely include innovative application as much as novel technology, leading to FOEs in which the possession of exquisite systems will not necessarily equate to mastery of the battlefield.

The convergence of digital, biological and physical technologies will reshape the FOEs, blurring operational boundaries. Joint, multi-domain and even civil–military activities will increasingly occur within a single, hyperconnected

information environment, reducing decision cycles from minutes to seconds. Forces will face continuous sensing and persistent surveillance from both high end and ubiquitous low-cost platforms, making concealment and manoeuvre significantly more challenging. Tactical surprise may therefore shift from physical disposition to digital manipulation, sensor deception and exploitation of automated decision loops, fundamentally altering how operational advantage is generated and protected.

Opportunities from cutting-edge science and technology will likely be balanced with potential obsolescence and reversion to legacy systems, and counter-technology measures. Obsolescence of systems and weapons may transform into a surprising form of resilience in certain futures. Counter-technologies and more responsive commercial capabilities may offer a viable and cost-effective alternative where immediate adoption of emerging or disruptive technology is not feasible. Sustaining existing major capabilities will increasingly sit alongside innovation and adaptability of those capabilities anchored around current and emerging scientific, academic and industrial expertise. Gradual adoption and integration of seemingly revolutionary technology may be more possible when working within the constraints of policy and regulatory frameworks.

The technological landscape of the FOEs will be defined by advances in data science, hyperconnectivity and AI, enabling seamless integration of human and machine-enabled decision-making. Military effectors are expected to become increasingly autonomous, precise, rapid and remote, fundamentally altering the character and tempo of operations.



Cyber: the invisible frontline reshaping warfare and global security thresholds

© Skorzewiak / Shutterstock.com

Cyber threats and quantum technologies will play a dual role – both enhancing operational capabilities and introducing new vulnerabilities that could compromise the FOEs. Similarly, breakthroughs in engineered biology and potentially geoengineering may offer significant benefits, such as improved resilience or environmental control, but also carry the risk of creating new classes of threats.

Dual-use technologies will become more prominent, obscuring the lines between conventional and strategic systems, making it harder to distinguish between civilian and military applications. The proliferation of novel and disruptive weapons systems will likely result in less explicit and more ambiguous technological arms races, complicating direct comparisons between adversaries and increasing the uncertainty of conflict outcomes.

This technological ambiguity will also transform escalation dynamics in 2040, where distinguishing hostile intent from routine commercial activity becomes increasingly challenging. Autonomous logistics swarms, commercial space constellations and civilian AI agents may create effects indistinguishable from hostile preparation. These blurred signatures heighten the risk of miscalculation and complicate the rules of engagement, particularly in congested space orbits, cyber and urban environments. As a result, future commanders will be required to manage competition, crisis and conflict simultaneously within overlapping, contested influence networks.

Ultimately, the convergence of these technologies will create FOEs in which advantage is transient, distributed and highly context-dependent. Success in 2040 may depend less on owning the most advanced technology and more on the ability to rapidly orchestrate diverse systems, degrade adversary networks and adapt faster than opponents across multiple operational domains and spaces. The FOEs of 2040 will have seen a shift from platform-centric to architecture-centric warfare, where modularity, interoperability and digital resilience has become the decisive factors shaping future campaigns.



Part 2

Disruptors

Section 1 – A snapshot of threat multipliers

Frozen conflicts. Historical tensions tied to identity, religion, ethnicity and nationalism may simmer below the threshold of conflict through unresolved border disputes, sovereign claims to territory and resources. Internal disputes over the distribution of power and wealth will likewise continue. Examples include: the disputes between China, Pakistan and India over Kashmir and Jammu; territorial disputes between North Korea and South Korea, Greece and Turkey, Egypt and Sudan; and conflicts over Western Sahara and throughout the Middle East. These frozen conflicts will provide fertile ground for malign actors, divert resources and create flashpoints that can rapidly escalate, drawing in regional or even global powers.

Migration. Large-scale and possibly overwhelming levels of migration will likely continue to strain social cohesion in host countries, which could increase competition over resources that fuel tensions and instability. Where deemed vulnerable, individuals could become targets for exploitation, as well as targets for aggression, especially where root causes are not understood or are misinterpreted. In circumstances where migration leads to social instability and tensions, the future operating environments (FOEs) may see military forces increasingly supporting border security, responding to humanitarian crises and augmenting stability.

Critical resources. Critical resources could increasingly influence conflict, security and military operations, as growing scarcity and uneven distribution heighten competition and volatility. The military's role in managing or mitigating the security implications of resource scarcity will likely expand. For military operations, resource scarcity could pose logistical challenges, especially maintaining supplies of water, fuel and food in resource-constrained environments. There might also be increased operational demand to secure access to these resources or to protect critical infrastructure associated with their extraction, production and distribution. Domestic security efforts may be expanded to secure or stabilise resource-rich regions abroad, particularly where scarcity intersects with weak governance or internal conflict. China's

dominance in processing and refining rare earths grants it significant geopolitical leverage, which it already uses to influence global markets. This may continue into the future if the issues of supply chain resilience are not addressed. As these changes gather pace, competition could easily escalate and risk new confrontation.

Geoengineering. Certain geoengineering technologies could raise concerns about unintended consequences of specific climate interventions by 2040. Cross-border impacts could destabilise regional climates, agricultural production and water resources. Nations without these geoengineering capabilities are likely to feel vulnerable to the actions of those that possess them, leading to a possible arms race in climate modification technologies. The transboundary nature of such activities complicates issues surrounding national sovereignty and will have far-reaching effects on neighbouring nations, challenging traditional notions of territorial integrity and self-determination. The lack of mutual agreement and governance frameworks increases the risk of international disputes.

Democratisation of intelligence. Commercial service models and the continued expansion of open-source material implies a potential democratisation of intelligence-related functions and capabilities. The abundance of easily accessible raw data will make it challenging to distinguish actionable insights from insignificant information and noise created to distract. Conflicts of interest are likely where providers supply multiple services to competing actors, both directly and indirectly. New commercial and ideological actors will enhance both collection and processing technologies and techniques. Some actors will use intellectual property of tools and information to gain political influence or primacy. Others may retain rights to adjust their use of data as situations or circumstances evolve, making them hard to mitigate or compete against. Decision paralysis due to unprecedented amounts of data or being seduced by selective use of evidence and confirmation bias will be a challenge. Disinformation and misinformation, along with acting unknowingly on assumptions, will complicate the picture.

Arms and technology races. Key novel and disruptive weapons systems and technologies mean the FOEs will likely be accompanied by less explicit and more ambiguous technological arms races. Steered by the desire to uphold their dominant standing and competitive edge, the United States, Russia and China will engage in recurring arms races of conventional, hybrid and strategic weapons, with middle powers struggling to keep up. Emerging powers are likely to accelerate conventional military investment to exert influence and

deter competitors and adversaries, and to broaden their ability to manage regional escalation. States embroiled in frozen historical conflicts over disputed territories will likely increase their military investment to maintain credible deterrence against opportunistic adversaries. For some states, the driver for military capability investment may be the international prestige and leverage brought by increasing military power

Nuclear, chemical and biological proliferation. Although the overall global inventory of nuclear weapons has declined over the last 30 years, the rate of decline is starting to slow, with the number of deployed warheads assigned to operational forces rising. Continued proliferation of strategic weapons could have cascading effects for arms control and non-proliferation norms, potentially triggering other states to pursue nuclear programmes of their own. Threats of chemical, biological and radiological weapon proliferation are poised to increase. The collapse of arms control may signal the start of intermittent rounds of vertical proliferation to increase the credibility of a nation's strategic forces that will lead to a new Nuclear Age. As security challenges grow more complex and new areas of conflict emerge, there might be opportunities for creative ways to regulate behaviours and set shared rules. Future arms control could focus more on managing the quality, effects and technology of weapons to prevent major gaps, rather than reducing numbers. However, efforts to limit the number of strategic warheads will remain integral to arms control.



© Anelo / Shutterstock.com

Redefining power: reach, risk and the race for dominance

Section 2 – A snapshot of novel and disruptive capabilities

Artificial intelligence. The potential further evolution from artificial general intelligence to artificial super intelligence is feasible by 2040. If artificial intelligence (AI) verifiably outperforms humans, the shift from human-in-the-loop to human-on-the-loop will extend onward to human-starting-the-loop. In some circumstances it may even reach a position of human-out-of-the-loop. Trust in AI will depend on its vulnerability to data poisoning, manipulation, sabotage and other types of attack, which could impair performance and lead to flawed decision-making or the misidentification of false threats. Any resulting distrust of AI could undermine communication between actors, enhance the risk of errors and premature reaction, and lead to inadvertent escalations. Countermeasures may involve deploying specific AI algorithms to detect and/or counter or deceive adversary AI systems (AI versus AI). This could create a dynamic and evolving challenge of distinguishing between AI, human and human-machine team-based decisions, and associated responses. While global adoption rates may vary, by 2040 the integration of AI will have demanded new approaches to human-machine teaming and ethical considerations in warfare.



Artificial super intelligence: challenging human control and public trust in the future of warfare

© Shutterstock.com

Quantum and post-quantum decryption. Quantum computing will likely render many extant encryption algorithms obsolete. Military forces will likely transition to quantum-resistant algorithms in response. Quantum decryption is anticipated to enhance intelligence gathering operations, offering decryption in real time. The ability to conduct this at scale risks significant exploitation of sensitive data with the growing use of decentralised networks making attribution very challenging. Although quantum key distribution and other similar technologies have the potential to address the security threats of quantum decryption, future forces will have to overcome significant technical barriers, including developing reliable quantum memory and quantum repeaters.

Autonomous and uncrewed systems. Uncrewed systems will continue to transform the way warfare is conducted. By 2040, they will extend far beyond their current role in support of intelligence, surveillance and reconnaissance, and individual strike missions. Air, land, maritime and space systems could become primary instruments of local superiority, particularly for precision strikes and air support to ground forces. Such capabilities will increase stand-off distances or enhance decoy and deception. They will also offer enhanced survivability in contested environments, increased persistence over target areas, improved force density and operate in high-risk scenarios – all while reducing threats to the human operator. These might be increasingly relocated from land to other environments, including maritime or even space. Swarm tactics, including the use of drones, AI-driven decision-support systems and autonomous weapons could overmatch human control over pre-conflict escalation management. The routine presence of autonomous and uncrewed systems could increase the risk of miscalculation and unintended escalation.

Electromagnetic warfare systems. Advances in electromagnetic surveillance and attack systems, including the proliferation of low-cost jammers and sensors, will increase the likelihood of the electromagnetic spectrum and spectrum-dependent systems being disrupted by a range of actors, including non-state actors. These electromagnetic warfare systems will have increased range and be powerful enough to exert high energy to penetrate, disrupt or destroy electronic systems. Adapting and fighting through electromagnetic warfare will likely involve not only defending against electromagnetic attacks but also using local jammers and inhibitors to enable force protection. Preventing targeting by denying the use of the electromagnetic spectrum to protect communications and navigation systems offers strategic advantage and enhances the ability to detect, deceive and disrupt adversary operations.

Directed energy weapons. The use of directed electromagnetic energy rather than kinetic energy will increase the precision of weapon effects against military targets. Directed energy weapons' ability to create speed of light effect with almost unlimited ammunition (as long as power supply and other technical issues are resolved) could enhance military postures, operational endurance and reach. They would be especially suited to fixed area denial and critical infrastructure protection where power provision is unconstrained. This would transform counter-strike capabilities, particularly against new, emerging or disruptive threats like hypersonic weapons or uncrewed swarm attacks.

Hypersonic weapons. Hypersonic cruise missiles and glide vehicles will improve the effectiveness of deep strikes due to the reduced detection and response times, which could provide a strategic advantage to the attacker. In some circumstances, this could affect decision calculus. Hypersonic glide vehicles will pose significant threats to fixed military installations, large platforms and concentrated troop formations, and may force a shift towards more dispersed and mobile force structures, thereby complicating future deterrence postures. Unless the cost per unit is lowered, hypersonic weapons are likely to be retained for use against the most important targets and strategic weapons, with potential relevance for deterrence calculations. This impact will be compounded by the pace of countermeasure development linked to other areas of disruptive technology.

Supercavitation. Parallel to advances in hypersonic weapons, further proliferation of supercavitating weapons will have similar disruptive effects in the future maritime and submarine operating environments. Supercavitating torpedoes travelling at extremely high speeds will likely drive changes in the way naval warfare tactics and mission planning are executed. Possession would enhance a state's ability to threaten maritime assets at greater distances with significantly reduced reaction time. Integration with multiple platform types may render many anti-torpedo capabilities obsolete, creating a deterrent effect.

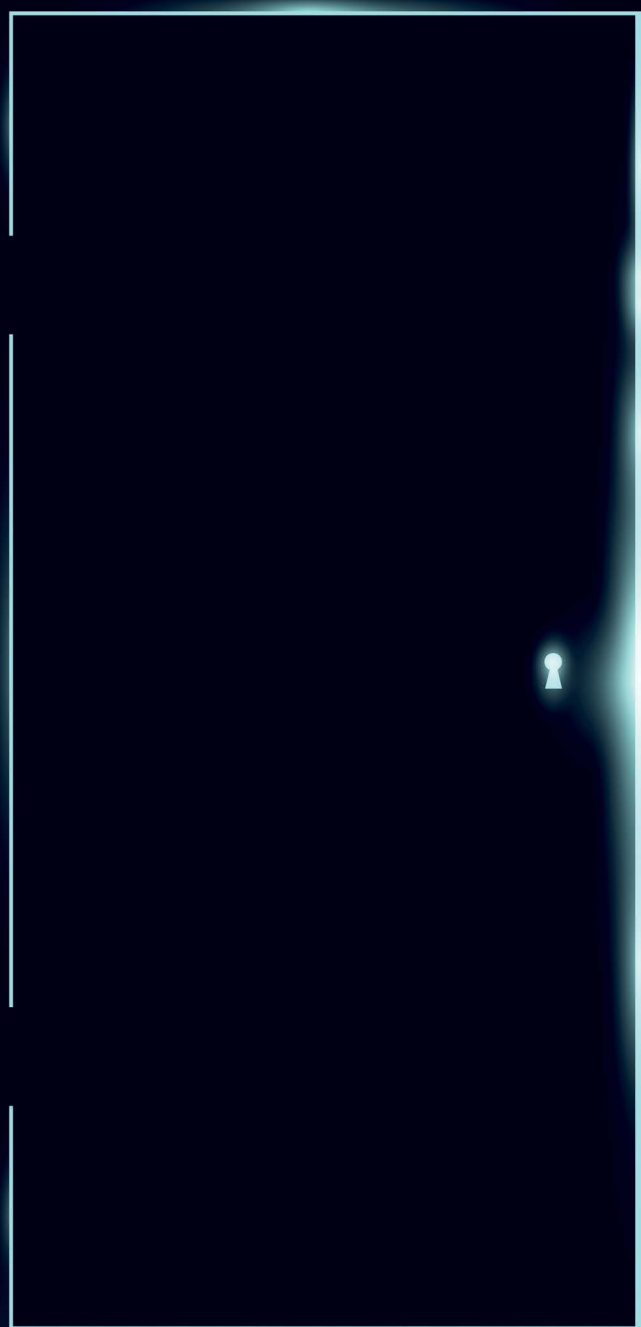
Engineering biology. Advances in biological sciences and engineering biology, combined with AI and data processing, could lead to capabilities that enhance or alter human physical and cognitive limitations. From enhancing the human microbiome to brain-computer interface technologies as part of human-machine teaming, the blending of these could present revolutionary advantages and threats. Technological convergence will almost certainly prompt further innovation. Potential areas include bio-enabled material science, sustainability (including recycling and remediation) and energy production and bio-enabled sensing. Advances in sustainability could

eliminate environmental footprints by achieving minimal operational waste. Bioengineering could also be used for the development of high-performance armour and corrosion-resistant material. These biomaterials could offer operational advantages, resulting in stronger, lighter and more adaptive military equipment.

Novel sensors. A combination of advanced military and civilian sensor systems, integrated with AI-enabled data fusion, has the potential to dramatically increase real time situational awareness. While increasingly sophisticated and pervasive sensor technology has been a historical constant, technological evolutions in the coming decades have the potential to disrupt operating environments and assumptions. Quantum radars, for example, could vastly improve detection of stealth aircraft. Despite existing (significant) physical and technological barriers, neutrino detectors have the potential to emerge as transformative technological disruptors with a wide range of strategic and operational applications. These trends will make the operating environment more transparent and reachable, reducing opportunities for manoeuvre.



Bio-innovation: transforming capability and risk



Key takeaways

Good bets

Key characteristics

- ✓ The future operating environments (FOEs) of 2040 will be congested and difficult to coordinate, command and control.
- ✓ It will be hard to maintain technological superiority.
- ✓ Integration across multiple platform types, and human and artificial intelligence (AI) capabilities will combine to outperform individual capabilities, which may create a deterrence effect.
- ✓ The evolving characteristics of FOEs will stretch today's meaning of homeland defence beyond physical and geographical boundaries.
- ✓ Growing and converging threats will blur homeland and external operations, and operational landscapes.
- ✓ Intelligence will be decentralised and increasingly democratised.
- ✓ Vertical nuclear proliferation will increase, with existing nuclear powers diversifying options and means.
- ✓ Key novel and disruptive weapons systems and technologies mean the FOEs will likely be accompanied by less explicit and more ambiguous technological arms races.
- ✓ Armed political and ideological factions could acquire access to even more capabilities previously restricted to states.

Good bets (continued)

Actors

- ✓ Increasing rivalry among major powers, and growing influence of regional and non-state actors, will likely destabilise the international order.
- ✓ Existing adversarial relationships will endure.
- ✓ States will likely remain principal actors, however, the number and type of security actors will rise.

Spaces

- ✓ Future warfare will extend and merge environments and operational domains: subsea and deep sea to subterranean and deep space, across the electromagnetic spectrum and throughout augmented, virtual and cognitive spaces.
 - The maritime operating environment will become increasingly accessible, visible and reachable.
 - Land operations will exist in cluttered, digitally connected and exposed conditions.
 - The speed of fielding and adaption will determine which air capabilities remain credible, resilient and relevant.
 - Data-centric warfare will be common.
 - The cognitive operating space will be ever more untrustworthy.
 - Consensus on acceptable thresholds and methods of response, including the use of armed forces, will be challenged.

Good bets (continued)

Disruptors

- ✓ The FOEs of 2040 will be revolutionary with rapid and radical technological change; they will also be evolutionary and rudimentary. Technologically, they will be shaped by data science, hyperconnectivity and AI with the seamless integration of human and machine-enabled decision-making.
 - AI will increasingly become a core part of military decision-making and quantum computing will likely render many encryption algorithms in use obsolete.
 - High-end electromagnetic surveillance and attack system capabilities with greater range and power should be expected.
 - Directed energy weapons will shift military postures, operational endurance and reach.
 - Hypersonic and supercavitating weapons will change the speed and range of engagements, expanding effects from any given location.
 - The convergence of advanced sensor systems and AI-enabled data fusion will make engagement spaces increasingly transparent.
 - Effectors will become more autonomous, precise, rapid and remote.

Probable bets

- Certain states cede power to commercial and private entities.
- Expanding threats cause actors to extend arrangements of existing alliances, driving cooperation and reducing conflict risk.
- Issue-based, unilateral defence and protectionism leads to aggressive conflict.
- Space is militarised and weaponised.
- Actors use advanced quantum decryption to intercept communications in real time.
- Advances in bioinformatics, bioengineering and AI overcome human limitations.

'High impact, low probability' bets

- ! Some megacities become military powers in their own right.
- ! Commercial and private actors become independent military or security actors.
- ! Actors respect established international law and introduce norms to regulate emerging and novel technology.
- ! Generalised space warfare breaks out.
- ! Striving for complete data and cyber sovereignty could lead to volatile virtual battlegrounds.
- ! Artificial super intelligence replaces artificial general intelligence and is differentially adopted.

Glossary

AI	artificial intelligence
E7	Emerging Seven
EU	European Union
FOEs	future operating environments
G7	Group of Seven
GST 7	Global Strategic Trends: Out to 2055
MOD	Ministry of Defence
NATO	North Atlantic Treaty Organization
SDR 25	Strategic Defence Review 2025
UK	United Kingdom
US	United States

--	--

Acknowledgements

Future Operating Environments 2040 benefited from a combination of individual and collaborative research. Responsibility for the final product lies with the Strategic Foresight Team but was much advanced by the efforts and help of others, some of whom are listed below. We are very grateful and look forward to future interactions.

- Futures, concepts and capability representatives from across UK Defence, including the Military Strategic Headquarters, Royal Navy, British Army, Royal Air Force, Space Command, and Cyber and Specialist Operations Command
- UK intelligence community
- Defence Science and Technology
- Defence Science and Technology Laboratory
- NATO, Allied Command Transformation strategic foresight
- United States Department of Defense, Directorate for Joint Force Development
- Canadian Department of National Defence, Foresight and Concept Development
- Ministry of Defence Singapore
- Japanese National Institute for Defense Studies
- Australian Department of Defence
- Brazilian Navy/Brazilian Navy Staff
- German Armed Forces/Bundeswehr Office for Defence Planning
- Finnish Ministry of Defence/Finnish Defence Research Agency
- Swedish Armed Forces and Swedish Defence Research Agency



