



Ministry
of Defence

Strategic Trends Programme
Future Operating Environment 2035



First Edition

WITHDRAWN



Ministry
of Defence

Strategic Trends Programme
Future Operating Environment 2035

WITHDRAWN

First Edition

WITHDRAWN

Conditions of release

The *Future Operating Environment 2035* comprises one element of the Strategic Trends Programme, and is positioned alongside *Global Strategic Trends – Out to 2045* (Fifth Edition), to provide a comprehensive picture of the future. This has been derived through evidence-based research and analysis headed by the Development, Concepts and Doctrine Centre, a department within the UK's Ministry of Defence (MOD).

This publication is the first edition of *Future Operating Environment 2035* and is benchmarked at 30 November 2014. Any developments taking place after this date have not been considered.

The findings and deductions contained in this publication do not represent the official policy of Her Majesty's Government or that of UK MOD. It does, however, represent the view of the Development, Concepts and Doctrine Centre.

This information is Crown copyright. The intellectual property rights for this publication belong exclusively to the MOD. Unless you get the sponsor's authorisation, you should not reproduce, store in a retrieval system or transmit its information in any form outside the MOD. This information may be subject to privately owned rights.





Contents

Introduction	vii
Chapter 1 Strategic context	1
The global context	1
The UK context	5
Global stress map: 2035	8
Chapter 2 Characteristics of the future operating environment	11
Actors	11
Institutions	12
Culture and identity	13
Technology	13
Cyberspace	20
Electromagnetic environment	20
Physical environment	21
Future legal aspects	25
Chapter 3 Implications for Defence	29
The challenge	29
The increased importance of the 'understand' function	30
Remote and automated systems	31
Access, anti-access and area denial	32
The urban and littoral challenge	32
Blurring of UK and overseas threats	32
Humanitarian assistance and disaster relief	33
Reconstitution	34
Agility	34
Conclusion	39
A commander's perspective: 2035	41
The '5Cs'	44
Acknowledgements	45



Introduction

Aim

The *Future Operating Environment 2035* (FOE 35) forms part of the Development, Concepts and Doctrine Centre's (DCDC) Strategic Trends Programme. DCDC is the MOD's independent think tank and, as such, FOE 35 does not represent the official position of Her Majesty's Government. It supersedes the 2010 *Future Character of Conflict* (FCOC) and aims to:

describe the characteristics of the 2035 operating environment to provide evidence-based insights that can inform future Defence capability development.

FOE 35 describes the potential characteristics of the future operating environment, and is designed primarily to inform UK Defence and security policy-makers and our Armed Forces more broadly. However, it is intended to have applicability across UK Government and agencies to help inform their understanding of the future operating environment in which we all (military, other UK Government departments, international organisations and agencies) may find ourselves operating in 2035.

Method

As part of DCDC's Strategic Trends Programme, FOE 35 uses *Global Strategic Trends – Out to 2045*, Fifth Edition (GST 5) as its foundation. Extensive contributions were garnered from across Defence, UK Government, think tanks, academics, non-governmental organisations and other UK and international institutions. Following gap analysis, additional directed

commissions were produced. Subsequent proactive engagement by DCDC with a broad range of contributors has provided essential peer review and challenge functions for this product in pursuit of robustness and resilience.

Scope

While FOE 35 aims to provide a long-term analysis of the key characteristics of the operating environment in 2035, the nature of 'futures' work is such that attempting to pinpoint when particular trends or characteristics will emerge is invariably problematic. Where this is the case, we discuss characteristics emerging out to, as well as in, 2035. Some characteristics of the future operating environment in 2035 are likely to be similar to those apparent today, but novel factors will emerge and some characteristics will become increasingly important in determining the future environment in comparison to today.

Chapter 1 outlines the principal factors identified in GST 5 that may drive the UK Government to employ the military instrument. Chapter 2 describes the key institutional, technological, cultural and physical characteristics likely to shape the operating environment in 2035. It places understanding people (the actors) and their motivations at the centre of our ability to achieve an understanding of the future operating environment. Chapter 3 identifies some of the key implications drawn from our analysis. This will enable us to assess future military utility and opportunities for Defence in 2035. Elements of both can contribute to Defence's future force development process.

The challenge

The challenge of looking 20 years ahead is significant but, like GST 5, this work does not seek to predict the future. Rather, it describes the characteristics of plausible operating environments, resulting from rigorous trend analysis. It seems likely that the future will be characterised by an increase in the rate and impact of some current global trends (in particular urbanisation, globalisation and inter-connectivity) and an increasingly complex, ambiguous and wide range of potential threats. The rate of change in some technological fields is likely to be particularly dramatic, which may have the effect of 'accelerating' the future towards us in certain fields. Equally, some trends may experience local reversal. The potential for unforeseen, disruptive events cannot be ignored. These events – or 'shocks' – have a low probability of occurring, but Defence must consider shocks because of the high impact they could have. This suggests that a premium should be placed on flexibility, adaptability and national resilience. Readers wanting more detail on thematic and geographic trends or on potential strategic shocks should refer to GST 5.

DCDC's previous publication, the *Future Character of Conflict*, described the 2014 joint battlespace as:

congested, cluttered, contested, connected and constrained.

While these descriptors endure, FOE 35 aims to provide a wider and more detailed analysis to inform future Defence capability development.

Exploitation pathway

This document sets out to provide context for policy-makers. It aims to inform the debate on the future and, therefore, wider conceptual force development. FOE 35 is intended to provide a baseline for experimentation, but not to constrain Commands in their thinking. Indeed, to innovate and adapt are two attributes that will greatly assist Defence and its people as they move into the future. Armed with a better understanding of the future through FOE 35, threats can be anticipated and opportunities seized.



Chapter 1

Strategic context

Introduction. DCDC's *Global Strategic Trends – Out to 2045*, Fifth Edition (GST 5) provides a vision of a world in transition out to 2045. There are likely to be significant challenges resulting from population growth, migration, greater demand for energy, climate change, continuing globalisation, rapid urbanisation and the exponential rate of change in some readily-available technologies. A combination of these factors may lead to challenges at home, as well as fragility and instability within the wider international system. It is crucial to understand these broad trends – and the way they combine – as they are likely to underline the principal reasons for deploying the military instrument as an element of a coordinated across UK Government, multinational response in the future. Chapter 1 outlines the key factors identified in GST 5 that are likely to set the context for UK Defence in 2035.

The global context

The global trends discussed in GST 5 could lead to tension, but where such trends collide, instability and conflict are more likely to occur (see pages 8-9). These trends may also reverse or develop in unexpected ways, and some could also have positive benefits for UK security, interests and prosperity. GST 5 provides a comprehensive insight into trends. The trends most relevant to the *Future Operating Environment 2035* (FOE 35) are detailed below.

Globalisation and interconnectivity.

The UK will be more interconnected than it is today, continuing to benefit from globalisation.¹ By 2035, disruptive events

¹ Financial Times. (2014), 'Lexicon'. Globalisation describes a process by which national and regional economies, societies, and cultures have become integrated through the global network of trade, communication, immigration and transportation.



An increasingly interconnected world

will have increasingly global consequences – requiring action from the international community. However, in particular circumstances, there may be significantly less time available for states and other actors to plan for, and respond to, global and regional events that emerge rapidly. Faster and more agile military responses may be called for, posing a challenge for policy- and decision-makers.

Shift in the balance of power. The centre of gravity of global economic power is continuing to shift, away from North America and Europe, towards Asia, resulting in a change in the balance of power and an increasingly multipolar world. While the US is likely to remain the world's leading military power in 2035, its military advantage is likely to be reduced and challenged increasingly by China. Other rising powers, such as Brazil and India, will take a strategic interest beyond their own regions in pursuit of resources. States such as Australia, Canada, Germany, Indonesia, Japan, Mexico, Nigeria, South Africa and Turkey all look likely to have increasing regional significance. Russia may continue to have a global impact through its trans-regional conduct, bolstered by its sheer size and military power. However, it is likely to be increasingly hindered by demographic decline, dated infrastructure and systemic challenges including corruption and poor governance. In an evermore globalised and interconnected world it is not only these powers that will exercise influence. Other

less economically powerful state and non-state actors will also aim to exert influence (for example, through sponsoring terrorism or cyber attacks). In 2035, the key global economic powers will be the US, China and the EU – with India rising rapidly – but only the US and China are likely to have the capability to dictate global events and potentially challenge world order.

Demography. The global population is likely to rise from the current 7.2 billion to between 8.1 billion and 9.4 billion by 2035.² The rate of growth will be slower in most developed states: in some, it may even decline. In developing states, rapid population increases and urbanisation may lead to instability. This could be exacerbated by age and gender imbalances that are likely to add to political and social tensions. In particular, a large male youth population in the Middle East, Central Asia and sub-Saharan Africa could provide a reservoir of disaffected young men more susceptible to radicalisation.³ Conversely, investing in education and healthcare could lead to job creation, economic growth and positive social development.⁴

Urbanisation. By 2035, the majority of the world's population is expected to live in cities, with many located on or near the coast.⁵ The greatest increases in urbanisation are likely to be in Asia (see pages 8-9). Developed cities will be very modern with well-functioning infrastructure and institutions as well as ready access to resources. However, due to the rapid rate of urbanisation, many suburban areas are likely to be shanty towns. Failed or failing cities could become the source of major security

2 UN Department for Economic and Social Affairs. (2012), 'UN (2012) World Population Prospects'.

3 Caprioli, M and Trumbore, PF. (2003), 'Identifying Rogue States and Testing their Interstate Conflict Behaviour'.

4 Lagarde, C. (2014), 'A New Multi-Culturalism for the 21st Century', The Richard Dimbleby Lecture.

5 UN Department for Economic and Social Affairs. (2007), UN World Urbanisation Prospects Database.



Some areas will struggle to cope with rapid urbanisation

issues. Often they will be located in areas prone to natural disasters and lack resilience due to poor infrastructure, scarce resources and ineffective or absent institutions and emergency services. Poor governance and inadequate institutions could allow violent and criminal non-state actors to flourish. Patronage systems – often viewed as counter to Western norms – will, in some areas, continue to provide vital services where formal governance is lacking.

Climate change. As a result of climate change, sea levels will rise and extreme climatic events are likely to increase in intensity, frequency and duration out to 2035, resulting in loss of life, physical destruction, disease and famine. Secondary effects may lead to migration, social unrest, instability and conflict that could affect the UK's interests. There is likely to be an increased need for humanitarian assistance to address greater and more widespread suffering. The military is likely to be more frequently engaged in providing assistance – albeit in a supporting role – alongside evermore capable non-governmental organisations. While the effects of climate change will be seen across the globe, developing countries will feel the economic and social impacts of climate change more keenly, as they are

unlikely to have the resources to mitigate its effects as successfully as more developed countries.

Resource scarcity. Demand for a range of natural resources is likely to increase over the next 20 years. Rising costs associated with this demand may lead to intolerable levels of inequality within, or between, nations. Climate change could put more pressure on the availability of drinking water⁶ and contribute to food shortages. As many states share the same water sources, scarcity and diversion of rivers may cause shortages and crop failure, resulting in famine, migration and possibly conflict. There may also be a scarcity of fossil fuels,⁷ rare earth elements and new 'high tech' materials.⁸ To overcome these shortages, exploration will occur in remote and challenging environments, requiring new and more efficient extraction techniques to be developed. These areas

The trends are clear: more people than ever before in history will be competing for scarcer and scarcer resources in poorly governed areas that lack adequate infrastructure, and these areas will be more and more closely connected to the global system, so that local conflict will have far wider effects.

Dr David Kilcullen⁹

6 Oxford Research Group. (2011), 'Competition Over Resources; Drivers of Insecurity and the Global South'.

7 International Energy Agency. (2012), 'World Energy Outlook'.

8 Department for the Environment, Food and Rural Affairs. (2012), 'Resource Security Action Plan'.

9 Dr Kilcullen, D. (2013) 'Out of the Mountains: The Coming Age of the Urban Guerrilla'.



Water scarcity – a possible source of conflict

are likely to require appropriate protection measures to ensure their security, and ultimately, their viability. Old grounds for extracting resources may also become profitable again as technology develops. The need to transport critical resources over long and sometimes conflict-prone areas or routes may increase uncertainty and tension between states. The need to protect these lines of communication, as well as to guarantee access to resources, may increase competition and act as a catalyst for intra- and inter-state conflict.

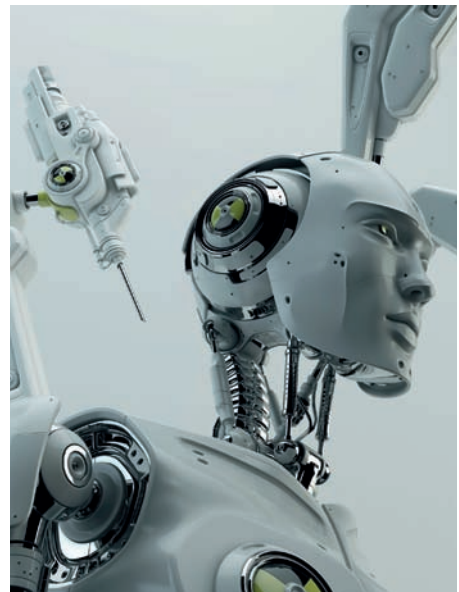
Corruption and criminality. Corruption undermines the proper functioning of governments by eroding their credibility, legitimacy and accountability. It can cause and perpetuate conflict and instability, and contributes to global inequality. Out to 2035, criminal transactions will increasingly use alternative currencies, making it easier to finance terrorist organisations anonymously. It will be more difficult than today for governments to freeze transnational criminal assets or sanction rogue regimes.¹⁰ Enforcing anti-corruption legislation will be challenging, especially in post-conflict states. Resistance to reforms may result in conflict or instability. Increased trafficking of drugs, weapons and people across porous borders will remain a worldwide security problem.

10 UK Ministry of Defence DCDC. (2014), 'Global Strategic Trends – Out to 2045, (Fifth Edition)', Strategic Trends Programme.

Better control measures at the national and international level will be necessary to increase transparency and reduce corruption.

Relationships with the state. There will be a broader spectrum of influential and empowered actors in 2035 who are likely to challenge the state more frequently on a variety of issues. These actors may range from small, grass-roots movements to large, well-connected collectives. Such actors will have a particularly noticeable effect in developing countries. While the state will continue to be the dominant actor in international affairs, large multinational corporations, non-governmental organisations and international organisations may be more prominent and influential.

Technology. Technology will be a key driver of change due to the rate of advance and growing accessibility in some fields. A novel approach to technology is also likely to provide opportunities to offset some sources of future tension. Globalisation of technology will lead to greater proliferation of lower-end equipment and a reduction in its cost, through economies of scale. This



Expensive high-end technology may make procuring sufficient numbers unviable

will allow a wider range of actors access to comparatively sophisticated weapons. Actors may employ existing dual use or commercial technologies in highly innovative ways, which may be disruptive. The previous technological advantage enjoyed by Western militaries will continue to be reduced out to 2035, for a number of reasons. Proliferation of technology means that a range of actors will have access to systems which used to be the sole preserve of developed countries. At the same time, Western countries are likely to be overtaken economically, meaning that they can be outspent on mass and capability. Furthermore, the West is unlikely to be able to rely entirely on high-end prime platforms to maintain its edge, as these look set to become considerably more expensive – making procurement of sufficient numbers unviable.

The UK context

The 2010 *National Security Strategy* states: 'The security of our nation is the first duty of Government. It is the foundation of our freedom and our prosperity'. It sets out a strategic approach to national security, summarised as follows:

- use all national capabilities to build prosperity, extend the UK's influence in the world and strengthen its security;
- use all the instruments of national power to prevent conflict and avert threats beyond UK shores;
- tie the efforts of all UK Government departments to address threats to national security and interests and to seek new opportunities for the UK; and
- be a prosperous, secure, modern and outward looking nation, confident in its values and ideas.

They will achieve this through:

- a commitment to collective security via a rules-based international system and key alliances; and
- a 'whole of UK Government' approach, based on a concept of security that goes beyond military effect.

Although the *National Security Strategy* will evolve over time to reflect the changing strategic landscape, its general themes and tenets are likely to endure.

Utility of the military instrument. The military instrument has a fundamental role to play in ensuring the survival of the state and the security of its citizens. The ultimate manifestation of this is its ability to fight the nation's wars – and war fighting remains the foundation of our national military capability. It also has a broader role in supporting our Government's wider interests and contributing to the nation's prosperity and stability through applying both hard and soft power.

To deliver both hard and soft power in pursuit of national security, prosperity and interests, the military instrument must be capable of fulfilling three overarching and interrelated functions, to:

- **protect** the UK mainland, our Overseas Territories and citizens abroad;
- actively **shape** the international environment to promote UK interests overseas and to enhance the UK's reputation and contribute to international security and stability; and
- **respond** to crises by projecting power to protect UK interests overseas and maintain international security and stability.

Although these three functions will remain relevant in the future, the way in which the UK uses the military instrument is likely to change, necessitating new approaches and capabilities. The balance of investment for each function will inevitably evolve to meet future challenges.

“

The art of war is of vital importance to the State. It is a matter of life and death, a road either to safety or ruin. Hence it is a subject of inquiry which can on no account be neglected.

”

Sun Tzu,
The Art of War



As we compete within a larger peer group, UK influence could decline

The UK in the international system. The UK has a vested interest in maintaining international organisations in which it plays an important role and wields significant influence.¹¹ The UK's relative influence could, though, decline out to 2035 as we compete within a larger peer group. However, our influence will continue to be bolstered by our system of government and our diplomatic, cultural and commercial weight, as well as the professional reputation of our Armed Forces. The UK has attributes that can be exploited despite the relative growth of other powers. Furthermore, the UK is likely to remain a significant global economy in 2035, possibly retaining its 2014 ranking as the world's 6th largest economy.¹² Continued access to established and emerging markets across the globe will remain key to the UK's economic prosperity. Any substantial disruption to globalisation, such as a major trading partner adopting significant protectionism, could have a severe impact on the UK economy.¹³

Rule of law. The UK will retain a vested interest in upholding state sovereignty and ensuring that countries adhere to international law. In areas where these rules are no longer observed, such as in failing states, human security¹⁴ and economic development will be jeopardised. The potential for violence in such areas may generate direct security threats for the UK at home and abroad.

Energy and resources. The UK will remain heavily reliant on imported energy, food and industrial resources. Our use of nuclear, as well as renewable sources of energy and alternative fuels, will increase out to 2035, but hydrocarbons will continue to form the backbone of our energy requirements. The security of trade routes along with the stability of the environments these resources originate from will remain vital. Our Armed Forces may be required to guarantee the security and supply of the UK's vital resources through deterrence, engagement or the application of force to defend against armed attacks.

11 Rt. Hon. Hague, W. (2010), 'Letter from Secretary of State for Foreign and Commonwealth Affairs to DSPG'.

12 Centre for Economic and Business Research. (2014), 'World Economic League Table'.

13 Dstl Policy and Capability Studies. (2013), 'Future Operating Environment 2035: UK Culture and Interests'.

14 Freedom from want, freedom from fear, freedom to live in dignity, <http://unocha.org/humansecurity/about-human-security/human-security-all>, accessed 2014.

UK soft power. Soft power is ‘the ability to affect others through the co-optive means of framing the agenda, persuading, and eliciting positive attraction to obtain preferred outcomes.’¹⁵ The UK has strong cultural, social and ethnic links across the globe – such connections will be invaluable if we wish to continue to use ‘soft-power’ as a tool for influence worldwide.¹⁶ This is manifest in the active role the UK plays within international institutions such as the United Nations (UN), the Commonwealth and European Union (EU). Our Armed Forces should expect to continue to contribute to the UK’s soft power in numerous ways as part of Government strategy, including Defence Engagement and when deployed on operations. Military soft power will have greater credibility if underpinned by hard power.

Population. In 2035, the UK is likely to have one of the largest populations in Europe, mainly due to immigration.¹⁷ The growing immigrant population may, if not integrated, strain social cohesion. However, positive demographic profiles will contribute to the potential for strong economic growth and boost the state’s ability to reconstitute military capability in times of crisis. Our Armed Forces will need to embody the diversity of the society they protect – a more diverse Armed Forces may be better able to operate in a globalised world where cultural awareness will be even more crucial than it is today. Building greater diversity will be particularly important in addressing growing recruitment challenges, generated in part by individuals feeling less connected to the state and, hence, less inclined to serve.

Blurring of the overseas and mainland threat. Greater interconnectivity may mean that, without mitigation measures,

critical infrastructure within the UK becomes increasingly exposed and vulnerable to remote attack, particularly from cyberspace. Borders will almost certainly be more porous by 2035, facilitating higher levels of migration. Larger immigrant diasporas are likely to maintain closer ties with their country of origin, through better communication links, such as social media. As a result, events abroad are likely to have a more direct impact at home. Military operations overseas may be influenced by the concerns of UK diaspora communities, such as the desire to provide humanitarian assistance to victims of a natural disaster from their country of origin. While it is possible that UK society may be less homogenous as a result of larger, better-connected diasporas (and the potential security challenges they may bring), a more globally-engaged population could also present significant opportunities.¹⁸

Public attitudes to operations. External scrutiny of the military (along with other public organisations) is likely to increase out to 2035. In liberal democratic societies, public and parliamentary opinion impacts military operations and governments’ willingness to deploy armed forces. When faced with a direct or existential threat, public and parliamentary opinion is likely to be resolute. But, when faced with more obscure, indirect threats to national security, interests and prosperity, public opinion can vary regarding so-called ‘wars of choice’. While current trends may suggest public unease with UK military intervention – with particular concerns over casualties, cost and longevity – such discomfort could reverse in the future. Shock events may change reticence overnight. Technology, such as automated systems, may also afford new opportunities.

“
Greater interconnectivity may mean that... critical infrastructure within the UK becomes increasingly exposed and vulnerable to remote attack, particularly from cyberspace.”

15 Nye, J. (2004), ‘Soft Power: The Means to Success in World Politics, Public Affairs’.

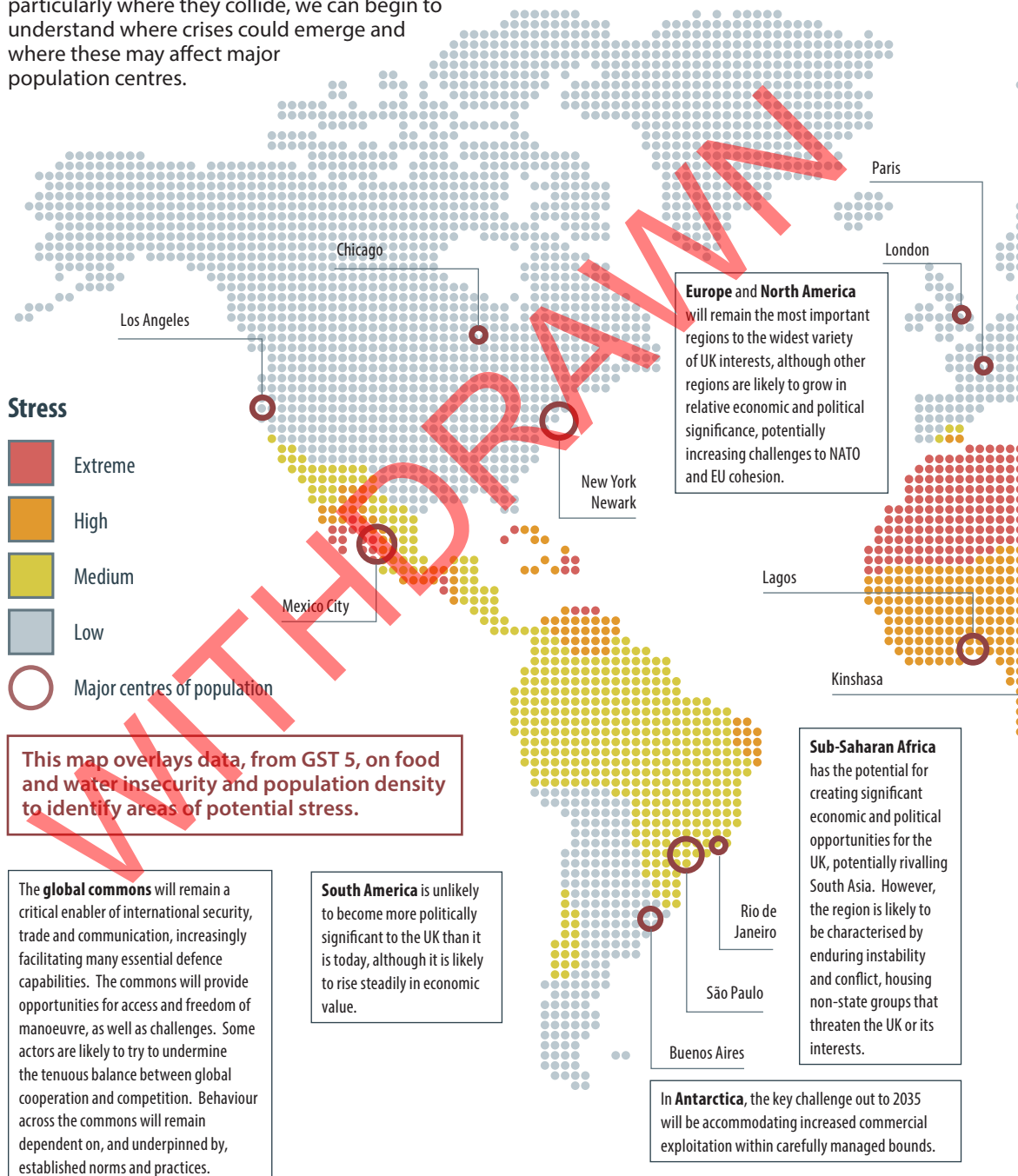
16 Barkawi, T and Brighton, S. (2013). ‘Brown Britain: Post-Colonial Politics and Grand Strategy’, International Affairs.

17 UN Department for Economic and Social Affairs. (2012), ‘UN (212) World Population Prospects’.

18 Barkawi, T and Brighton, S. (2013). ‘Brown Britain: Post-Colonial Politics and Grand Strategy’, International Affairs.

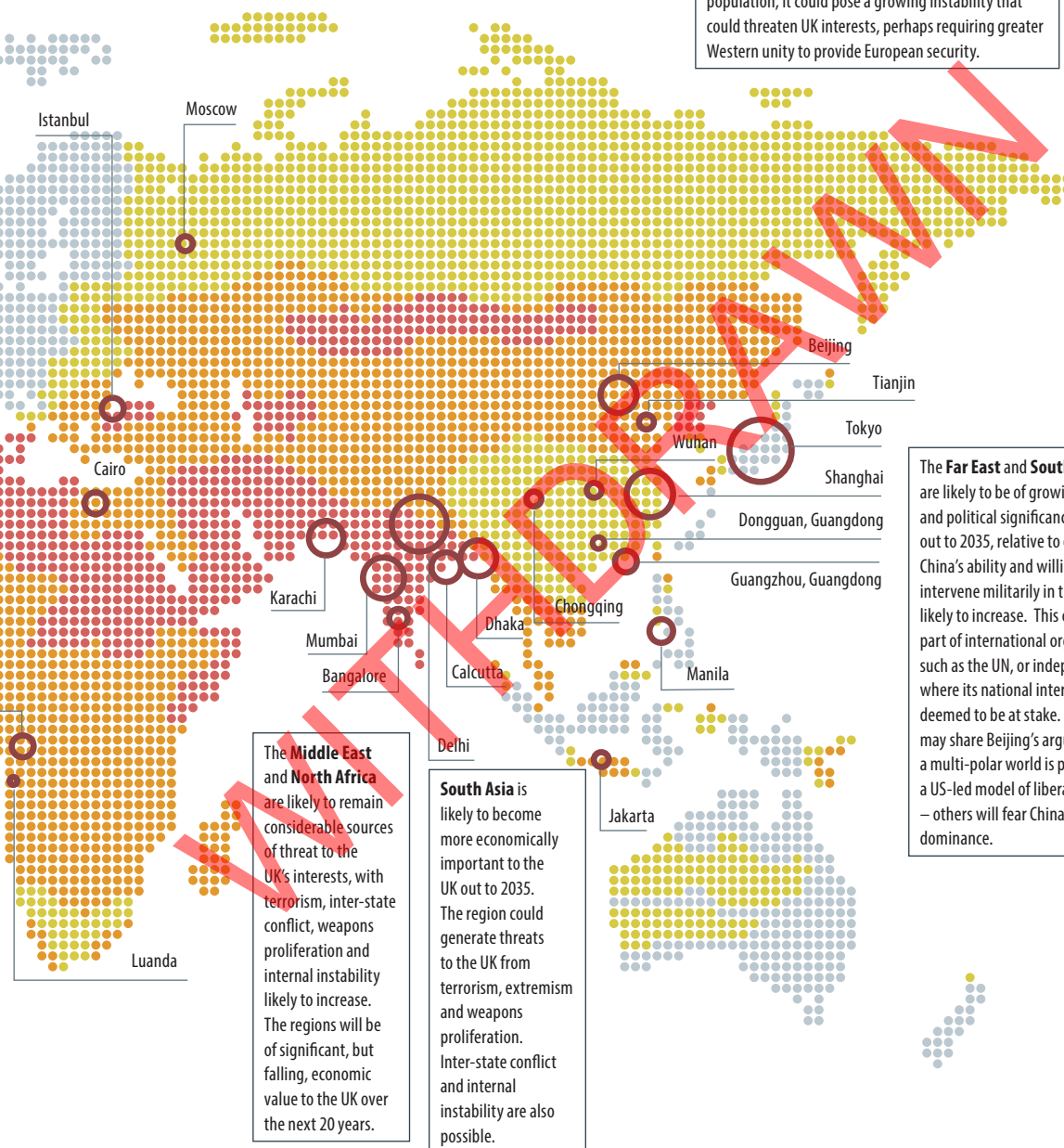
Global stress map: 2035

It is impossible to predict when and where humanitarian disasters, instability or conflict will occur. However, where global strategic trends are most likely to materialise, and particularly where they collide, we can begin to understand where crises could emerge and where these may affect major population centres.



As **Arctic** sea ice retreats, more shipping routes are likely to open up, along with greater opportunities for resource exploitation. This commercialisation could drive conflict, although large-scale military confrontation is unlikely. Governance arrangements could come under greater scrutiny, although significant change is not likely to occur by 2035.

Russia is likely to remain of geopolitical significance out to 2035. Despite its declining economy and ageing population, it could pose a growing instability that could threaten UK interests, perhaps requiring greater Western unity to provide European security.



Chapter 1 – Key points

- Increased globalisation may mean that states and individuals have significantly less time to plan for, and respond to, global and regional events that emerge rapidly. Faster and more agile military responses may be called for, posing a challenge for policy- and decision-makers.
- The US is likely to remain the world's leading military power in 2035, although its military advantage is likely to be challenged increasingly by China.
- By 2035 the majority of the world's population is expected to live in cities, with many located on or near the coast. These areas will often be prone to natural disasters. Failed or failing cities could become sources of major security issues: such cities may lack resilience due to poor infrastructure, lack of resources and ineffective or absent institutions and emergency services.
- The effects of climate change are likely to drive an increased need for humanitarian assistance to address greater suffering, suggesting that the military will more frequently be used to provide assistance – albeit in a supporting role – alongside capable non-governmental organisations.
- The need to protect lines of communication, as well as to guarantee access to resources, may increase competition and act as a catalyst for intra- and inter-state conflict. This will be important to the UK, which will remain heavily reliant on imported energy, food and industrial resources.
- There will be an increasing range of empowered actors in 2035, although the state will continue to play a dominant role in international affairs.
- Growing proliferation will allow a wider range of actors to access more sophisticated weapons, while the previous technological advantage enjoyed by Western militaries will continue to be reduced.
- The UK's relative influence could decline out to 2035, as it competes within a larger peer group.
- UK Defence is likely to have a broader role in supporting the Government's wider interests and contributing to the nation's prosperity and stability by applying both hard and soft power.
- Events abroad are likely to have a more direct impact at home, and military operations overseas may be influenced increasingly by UK mainland security needs.
- Critical UK infrastructure may become increasingly vulnerable to remote attack, particularly from cyberspace.



Chapter 2

Characteristics of the future operating environment

Introduction. Operating successfully in future environments requires a detailed understanding of their likely characteristics. Identifying influential trends early will help decision-makers plan more effectively for the future. Chapter 2 identifies the main actors and key characteristics that are likely to shape the operating environment in 2035. Many of these characteristics will increase the potential for instability and conflict, while others will offer opportunities for developing a more stable and balanced world.

Actors

State actors. The nation state will endure over the next 20 years and beyond, remaining central to the international order in 2035. Adaptable states are more likely to be successful, needing to interact increasingly with a variety of evermore influential non-state actors, international organisations and even super-empowered individuals. In 2035 there is likely to be

growing competition between states for access to, and influence over, ever-scarcer resources. Whilst traditional state-on-state conflict cannot be ruled out over the next 20 years, state-sponsored terror attacks, use of proxies and cyber attacks are more likely.

Non-state actors. By 2035, some non-state actors – multinational corporations, non-governmental organisations and city authorities – are likely to be more influential than they are today, having a greater impact on world affairs. Cooperation between state and non-state actors will sometimes be essential, with three-way engagement between militaries, non-governmental organisations and multinational corporations becoming increasingly important. Given trends towards greater and more complex urbanisation, engagement with city authorities will be particularly relevant for urban operations.

Extremist non-state actors, often driven by ideological and criminal concerns,



The increasing diversity of non-state actors will make the operating environment more complex

will also persist. By 2035, extremists will almost certainly be more able to exploit information technologies, with the potential to significantly disrupt communication and economic links. Extremists may also be able to employ a wider array of military capabilities (albeit on a limited scale), using innovative tactics that exploit our inherent vulnerabilities, including any institutional inertia. They are likely to develop ever-higher levels of lethality to counter our protection systems and may even have access to weapons of mass effect. To achieve continued impact, extremist non-state actors may seek to deliver progressively more 'spectacular' and violent acts that ultimately lead them to be alienated and isolated. However, where successful, these may cause mass casualties on a scale not yet seen,¹⁹ with significant economic, social and institutional impact. The links between extremist non-state actors and more powerful criminal organisations are likely to be maintained. Distinguishing between criminals and terrorists may become more difficult over the next 20 years.

Institutions

Alliances and partnerships. Working within international organisations, or with allies and partners, is likely to remain the preferred method of international engagement for the UK in 2035. The importance of such partnerships will grow, but they are likely to change in construct and character, resulting in a more complex and ambiguous international environment where there is greater alliance variability. 'Partnerships of the willing' or bilateral alliances, such as the US-Japan Defence Alliance, are likely to become more prevalent – particularly for specific operations and perhaps as a subset of larger alliances. For the UK, NATO will remain the defence alliance of choice – providing the continued commitment to Article 5 (collective self-defence of member states) but also the means of interoperability with a wide range of nations that could form coalitions of the willing. A shift in UN Security Council membership may occur by 2035, perhaps with additional members reflecting the shifting balance of power. The UN is likely to

¹⁹ Hoffman, B. (1993), 'Holy Terror: The Implications of Terrorism Motivated by a Religious Imperative'.

work through regional organisations²⁰ – such as the ASEAN (Association of South-East Asian Nations) – to achieve its aims, including a greater role in upstream conflict prevention. The need for large-scale UN operations – perhaps in Africa – and UK involvement in (and possible leadership of) them should not be discounted. The EU is also likely to continue to play a greater defence and security role.²¹ Interoperability and adaptability will be key as bespoke alliances and partnerships are formed, both between nations and with non-state actors (such as governments working with non-governmental organisations to deliver humanitarian relief).

Culture and identity

By 2035, identity may be more dependent on culture and ideology than geography. The ongoing growth and proliferation of social media, and evermore rapid spread of ideas, will create new forms of identity-based ‘turbulence’ or volatility, which gain strength by their associations. This is likely to intensify, complicating battlespaces by broadening audiences and energising ‘causes’ for which people fight, and for whom pragmatic compromise will be harder to accept. All actors are likely to exploit social media’s readily-available open-source intelligence-gathering advantages for control, recruitment, manipulation and targeting. Extreme religious and nationalistic ideologies are likely to characterise the future operating environment more often.

Religion. Faith-based ideologies will continue to shape many conflicts around the world and will remain an organising force in 2035.²² More extreme religious ideals will tend to make wars longer and more violent, especially where religious sites are co-located with valuable natural resources.²³

By 2035 extreme religious networks are likely to be increasingly global²⁴ and will often play a greater role in channelling transnational support to ideologically-driven conflicts.

Nationalism. Nationalism and national identity will be a significant, albeit reducing, driver of conflict out to 2035. Tensions arising from differences of nationality and culture²⁵ and a rise in ‘identity politics’ will carry a high risk of sectarian or communal violence.²⁶ This will be especially true where dominant national identities continue to suppress weaker ones. Globally, armed forces may be engaged in more areas where the challenges of both national and transnational allegiances are present.

Social and behavioural intelligence.

Technological advances are likely to mitigate some of the inherent challenges associated with understanding human behaviour and activity. Analysis and predictive modelling of social behaviour will increasingly support operations.²⁷ Analysis and visualisation techniques will be reliant on social media intelligence feeds,²⁹ including tactical information gathering. Such intelligence will guide and support decisions, including targeting, across the spectrum of conflict. It may also help us to understand human behaviours across social networks, as well as providing opportunities to influence them.

Technology

Technology will remain an essential and pervasive element of the future operating environment and a key driver of military change over the next 20 years. Increasingly, defence and security systems will rely on exploiting commercial research and

“In an environment defined by the intermingling of friends, enemies, and neutral parties, understanding social and cultural networks becomes just as important as the weapons we employ.”

Gen. Ray Odierno,
US Army²⁸

20 UK Ministry of Defence NATO and European Policy (NEP). (2013), ‘The UN’.

21 UK Ministry of Defence NEP. (2013), ‘The EU’.

22 Gutowski, S. (2013), ‘Religion and Security in International Relations Theories’. The Routledge Handbook of Religion and Security.

23 Toft, M.D. (2007), ‘Getting Religion: The Puzzling Case of Islam and Civil War’, International Security.

24 Roy, O. (2004), ‘Globalized Islam: The Search for a New Ummah’, Columbia University Press.

25 Hechter, M. (2000), ‘Nationalism and Rationality’, Journalism of World Research Systems.

26 The Japan Times, (2013), ‘Nationalism, Tibetans and Uighurs in Today’s China’.

27 Lock, R, Uttley, M and Lyall, P. (2011), ‘Honing Defence’s Intellectual Edge’.

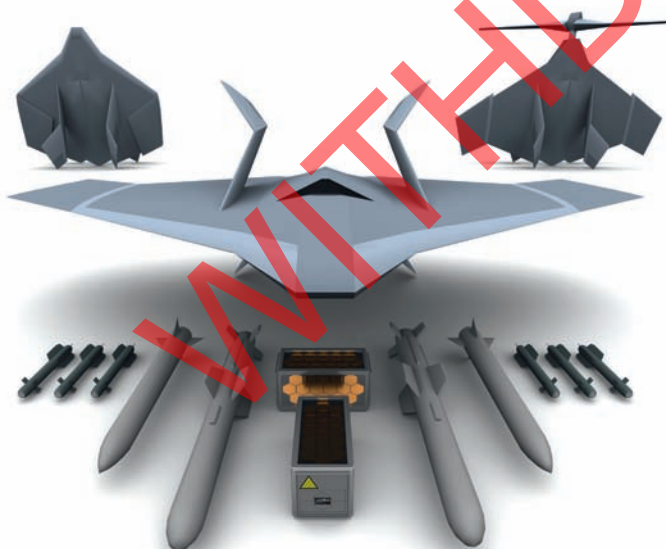
28 Gen. Odierno, R. (2013), ‘The Force of Tomorrow’.

29 Canna, S. (2013), ‘Operational Relevance of Behavioural and Social Science to DoD Missions’.



//
New
technology
needs to be
increasingly
adaptable.

innovation.³⁰ Sharing knowledge amongst diverse communities will also lead to innovative, break-through technologies – some of which may be game-changers.³¹ Increasing competition to maintain technological advantage may also prompt a sudden ‘technology jump’ leading to strategic or operational shocks.



30 FitzGerald, B. and Saylor, K. (2014), ‘Creative Disruption: Technology, Strategy and the Future of the Global Defense Industry’.

31 McKinsey Global Institute, (2013), ‘Disruptive Technologies: Advances That Will Transform Life, Business & the Global Economy’.

The changing technological landscape

The technological challenge. Technology developments will offer our Armed Forces opportunities as well as posing challenges. Gaining and sustaining military technological advantage will be increasingly challenging out to 2035, although some states may achieve temporary dominance in particular areas. Pressure on defence budgets, weapon proliferation and adversaries who choose to focus their capabilities in specific environments will all be contributing factors. As a result, by 2035, the UK and other Western militaries, probably with the exception of the US, will almost certainly have been overtaken in some technologies, and may need to become accustomed to being overmatched by derived capabilities.

Proliferation. Global connectivity and open markets will facilitate greater access to research, equipment concepts and technologies. Along with decreasing production costs, these factors will enable technologies to proliferate, allowing a diverse range of actors to access capabilities once restricted to just a few states.³² A range of actors, including less advanced adversaries, may employ existing dual-use or commercial technologies in highly innovative ways that may dislocate our understanding of their activity. Additive manufacturing (sometimes referred to as 3D printing), reverse engineering and greater innovation will increase the amount of illicit and unregulated technology transfer, exacerbating the threat to the UK. Other actors will access, adopt and integrate technology at a rate that will make it increasingly difficult for the UK to maintain a technological edge.

Tempo. The rate of technological change will accelerate out to 2035, serving to highlight inadequacies in less adaptable procurement processes within Defence. Civil companies will be able to raise revenue far more quickly, driving technology development in new directions and at faster rates. Over the next 20 years, militaries are

32 Krepinevich, A. (2011), ‘Get ready for Democratization of Destruction’.

likely to find it more difficult to maintain capability levels, unless new technology is quickly and affordably integrated. This tempo may mean that our capabilities have a shorter service life as countermeasures are developed more quickly, requiring a regular refresh to maintain advantage.

Adaptation. New technologies will need to be increasingly adaptable out to 2035 – both to allow for interoperability with legacy systems and for modernisation or upgrade. Simply procuring superior capability will not be enough – the speed at which Defence can adapt and integrate technologies will be more important.^{33, 34} Maximising cross-environment utility will also be an important consideration for military equipment. In future, the UK may be obliged to share with, and use, allies' intelligence and cutting-edge technology to enhance interoperability and effectiveness.

Key technological capabilities

Anti-access and area denial capabilities.³⁵

By 2035, proliferation of anti-access and area denial capabilities will enable a wider range of potential adversaries to deploy weapons to deny our access to, and freedom of movement within, operational areas. The aim of our adversaries is likely to be to deter Western powers by raising the potential cost of action.

Anti-access is intended to exclude our Armed Forces from theatres or limit their effective use and transit of the global commons. In the broadest sense, anti-access may involve political and economic exclusion, which in military terms could translate into refusal for basing, staging, transit or overflight rights. Under more hostile circumstances, lethal anti-access systems in 2035 will include evermore sophisticated longer-range



capabilities such as:

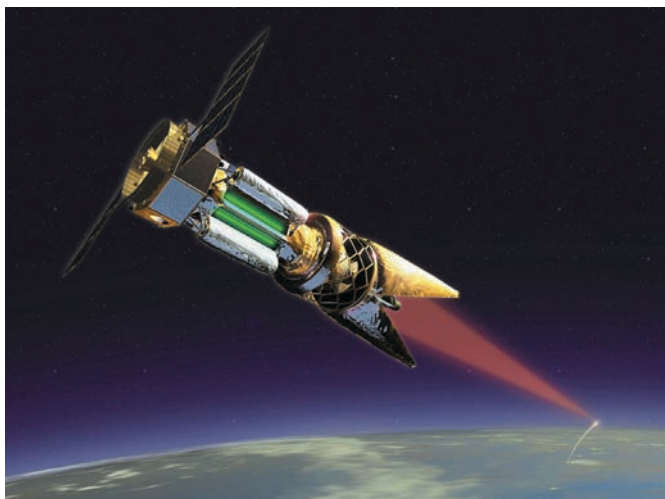
- ballistic missiles (conventional warhead);
- loiter-capable automated systems;
- anti-ship ballistic missiles;
- super-cavitating torpedoes;
- advanced (perhaps even unmanned) submarines; and
- weapons of mass effect.

For more advanced actors, offensive space- or ground-based anti-satellite systems will be able to disrupt the UK's own space assets. Offensive and defensive cyber capability will offer specific advantages – disrupting our networks and systems, while countering our offensive cyber operations. Less technical methods will include conventionally-armed terrorist attacks and proxy warfare methods that open alternative fronts. Such methods

33 US Defense Science Board (2013), 'Technology Innovation Enablers for Superiority in 2030'.

34 Miller, M. J. (2014), 'Statement by Deputy Undersecretary of the Army for Research and Technology'.

35 Extracts in this section from Freier, N. (2012), 'The Emerging Anti-Access/Area-Denial Challenge', Center for Strategic and International Studies.



Novel weapons: future ballistic missile defence?

are likely to distract both our resources and attention away from the areas the UK is trying to access, while seeking to impose excessive political costs for decision-makers. Acute, sophisticated and comprehensive anti-access challenges are likely to be most evident in Asia, but by 2035 weapon proliferation and technological advances will mean the threat is increasingly global, and more potent.

Area denial threats are also likely to impact heavily upon both political and military risk calculations. The coordinated and networked use of both high- and low-end technologies in a multilayered approach will limit or deny our ability to project power, and sustain and protect our fielded forces – they will present a prolific barrier to effective theatre entry and operation. Lethal and disruptive area denial threats will manifest most often at close range, attacking our vulnerabilities in all environments. Initially, they create physical resistance to theatre entry and then limit the freedom of manoeuvre of forces in theatre. In 2035, lethal area denial capabilities will range from the crude to the increasingly sophisticated. Methods will include:

- more readily available and advanced cruise and ballistic missiles;
- weapons of mass effect;

- target-specific mines;
- guided and kinetic munitions;
- directed energy weapons;
- increasingly effective and longer-range man-portable air defence and anti-armour systems;
- automated weapon systems; and
- swarm tactics.

Remote and automated systems. Remote and automated systems,³⁶ including those that are armed, will proliferate over the next 20 years. As they become cheaper and easier to produce, technologically advanced systems are likely to proliferate, with developing states and non-state actors having growing access to capable systems.

While initially the questions surrounding new automated systems may limit their use when there is a low appetite for risk, as capabilities become more advanced and more trusted, their use is likely to become commonplace. The level and nature of human control of remote and automated systems will be key. By 2035, it seems likely that automated systems will be advanced and highly adaptable. Low-end systems with limited mission-sets will retain the advantages of low cost, rapid procurement and quick adaptation to the challenges of the operating environment. Advances in technology will almost certainly enable swarm attacks, allowing numerous devices to act in concert. This may serve to counter the advantage of high-end systems. Western militaries are likely to insist on humans continuing to make decisions on the engagement of targets by automated systems, but some of our adversaries may not be bound by, or follow, the same legal and ethical constraints.

³⁶ 'Remote' and 'automated' capabilities are often taken to be interchangeable. However, an important distinction is that automated systems need not operate at range, and remote capabilities need not be automated (they could be controlled, at a distance, by a human operator).



The potential use of tactical nuclear weapons will complicate deterrence

“
... a range
of state
actors may
use tactical
nuclear
weapons
as part of
their strategy
against
non-
nuclear and
conventional
threats...
including
severe cyber
attacks.
”

Novel weapons. By 2035, the majority of missiles (including anti-ship cruise missiles) will operate at supersonic or even hypersonic speeds (five times the speed of sound or greater), with new technologies designed to defeat advanced electronic countermeasures. They are likely to have increased survivability aids through stealth technologies and alternatives to global positioning systems (GPS). Some weapons may be limited in range and the advantage offered by high speed may be negated by countermeasures such as directed energy and electromagnetic pulse weapons. Gun systems are likely to incorporate electromagnetic rail gun and hybrid explosive technologies, allowing a large number of smart munitions to be delivered with greater precision and lethality.

Cheaper, faster and more effective missiles will continue to drive a revolution in missile defence capabilities. Further, growing intolerance towards civilian casualties and demand for increased levels of accountability will drive the need for greater distinction, precision and proportionality. As a consequence, our Armed Forces will need to exploit directed energy weapons such as high-powered lasers.^{37, 38} The current

barriers of power generation and storage for these weapons will almost certainly have been overcome by 2035. Radio frequency or microwave emitters will also be capable of delivering energy on personnel to cause lethal and non-lethal effects. Militaries will need to protect their own systems and personnel against disruption by these weapons, as the threats from these weapons rapidly emerge.³⁹

Nuclear weapons. There are currently nine independent nuclear weapon states holding some 17,300 warheads (down from 68,000 in 1985) although only the US and Russia have more than 300.⁴⁰ Despite reductions, nuclear states are almost certain to continue to modernise their capabilities out to 2035 and remain committed to retaining nuclear weapons. Assessments of whether particular actions warrant a nuclear strike may differ between actors. Some commentators believe it is increasingly likely that a range of state actors may use tactical nuclear weapons as part of their strategy against non-nuclear and conventional threats

37 Boeing Counter-electronics High-powered Microwave Advance Missile Project.

38 UK Ministry of Defence, Dstl. (2014), 'Novel Weapons programme', www.gov.uk/government/publications/novel-weapons-programme.

39 House of Commons Defence Committee. (2012), 'Developing Threats: Electro-Magnetic Pulses (EMP) Tenth Report of Session 2010–12'.

40 Federation of American Scientists, (2013), 'Status of World Nuclear Forces'.

“
The likelihood of terrorists succeeding in attacks that cause real mass destruction will remain low.”

coming from any environment, including severe cyber attacks.^{41, 42} Limited tactical nuclear exchanges in conventional conflicts by 2035 also cannot be ruled out, and some non-Western states may even use such strikes as a way of limiting or de-escalating conflict.

If isolated military targets are subject to nuclear attack, any land-based nuclear response could be seen as an unjustified escalation, in light of the nature of the weapon, civilian casualties and its impact on the environment. Future threats may also come from groups who – due to their dispersed locations – cannot be the subject of a nuclear counterstrike, such as terrorists or cyber criminals. Of note, illicit nuclear trade is likely to continue out to 2035 and preventing nuclear proliferation is likely to require greater international consensus and political will.

Other weapons of mass effect. The likelihood of terrorists succeeding in attacks that cause real mass destruction will remain low. If terrorists do use weapons of mass effect in the future, attacks are likely to be chemical, biological or radiological – and could even be nuclear.⁴³ Weapons of mass effect will be under continued international surveillance but future limited tactical use by rogue regimes or ideologically driven non-state actors cannot be ruled out. Future developments may include the targeted spread of disease and use of nanotechnology. For example, nano-sized carbon particles could be used to cause severe respiratory problems.⁴⁴

Exploiting technical advances

By 2035, many of today's key emerging technologies will have a major impact across Defence. Some capabilities may have a disruptive effect, while other technologies

may experience step changes in their development, emerging from combinations of individual technical advances, rather than from a single specific field. In particular, advanced materials, additive manufacturing, power and energy technologies, and developments in life sciences could have a profound effect on military capability. Advanced materials will possess new physical, thermal and chemical properties while offering the ability to manufacture at the nano-scale. This will allow us to create new structures and to integrate capabilities at ever smaller, cheaper and effective scales. They will also offer advantages of protection, reduced weight, deception and repair through self-healing. Additive manufacturing will make our logistics chain lighter.⁴⁵ This will be key to operating in non-permissive environments, especially when the support chain is long, expensive or threatened. It may also allow individuals, non-state actors and developing states to produce very large numbers of cheap, precision weapons. Research in power and energy generation and storage could create smaller, lighter and more durable batteries. This will lessen the physical burden on our personnel and further reduce the logistics burden to extend our operational reach.

By 2035, physical and cognitive performance will be artificially enhanced via biomechanical systems such as exo-skeletons or prosthetics, wearable devices and sensors, and memory-enhancing drugs. Synthetic biological components will enable new substances to be developed. But such advances could also lead to new pathogens being deliberately or accidentally created and released, potentially causing or exacerbating pandemics. By 2035, it may even be possible to create genetic weapons.

Quantum technologies. Although a breakthrough will not necessarily occur in the next 20 years, quantum technologies promise a vast increase in processing capabilities and secure communication, particularly for encoding and deciphering sensitive messages

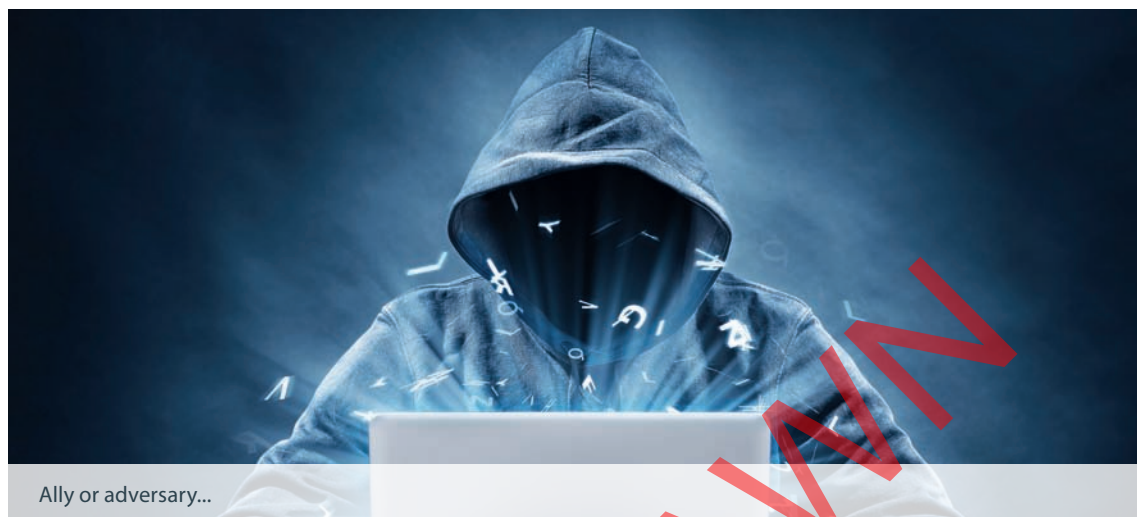
41 Hedenskog, J. and Vendil Pallin, C. (2013), 'Russian Military Capability in a 10 Year Perspective'.

42 Main, S. J. (2010), 'The Mouse that Roared or the Bear that Growled?'.

43 Mauroni, A. (2010), 'A Counter-WMD Strategy for the Future'.

44 Forest, J. J. F. and Howard, R. (2012), 'Weapons of Mass Destruction and Terrorism'.

45 Middleton, A. J. (2013), 'Additive Manufacture – Impact on MOD's Logistics from 2013-2035'.



Ally or adversary...

and signals analysis. Quantum technologies may also lead to improvements in precision sensing, allowing the visualisation of objects and voids in subterranean locations or behind obstructions. This will drive changes to stealth. Other developments are likely to include precision-timing devices that will enhance communications and global positioning.

Information and communications

Out to 2035, our Armed Forces will continue to rely on information and communications for: operations; political support at home; and strategic influence around the world.

Information and communications technology.

Information systems development will be increasingly driven by the commercial sector. By 2035, computers will more frequently connect, collect and share data with other devices seamlessly and without human intervention or (in some cases) knowledge – the so-called 'Internet of Things'. Practically unlimited data storage will be available on micro-scale devices, driven by the growing volume of digital data. Defence will need to continue to understand the impact on privacy, assurance, jurisdiction and security for data stored on any foreign-based servers. Such data servers will become an important part of critical national infrastructure, but may not have the type of protection afforded by UK sovereignty.

Big Data analytics. The opportunities provided by the growing volume of data will increase, as will the risk of information overload. Big Data analytics (the ability to collect and analyse a vast amount of information quickly) will become increasingly important and sophisticated over the next 20 years. Organisations, including non-state actors, will seek to gain information advantage. Like many state actors using Big Data analytics, they will be able to uncover patterns and correlations to create probabilistic forecasts. By 2035, language processing, anomaly detection and visualisation tools will be far more prevalent and will identify activities and trends much earlier than conventional techniques.

Surveillance. By 2035, persistent real-time, multi-sensor surveillance capabilities will be ubiquitous, cheap and passive, offering considerable advantage to a range of actors. This will have significant implications for operational security and counter-surveillance techniques. Surveillance capability is likely to be exploited through sensors distributed across all environments, including space. Surveillance throughout cyberspace will be increasingly evident. By 2035, sensors will be integrated with weapon delivery systems that track multiple targets.

//
...cyberspace
will be
ubiquitous
by 2035,
pervading
every aspect
of the physical
environments
to a far higher
degree than
today.

//

Cyberspace

FOE 35 considers cyberspace as a separate entity purely to emphasise that it will be ubiquitous by 2035, pervading every aspect of the physical environments to a far higher degree than today. Cyber operations and awareness must be considered as mainstream activities. In effect, cyber operations are part of the all-arms battlespace. As military systems become increasingly dependent on information networks (particularly to integrate sensors, weapons and command and control), cyber protection and resilience will be essential. Any use of cyberspace that impacts critical national and international infrastructures could result in military responses.

The global nature of cyberspace. The number of entry points and its decentralised and dispersed nature will mean that cyberspace is likely to remain porous and vulnerable to disruption. Cyberspace infrastructure is often situated in sovereign territory with dispersed ownership, particularly for space-based and cloud storage overseas. Although states may be both capable and willing to exercise jurisdiction over these areas, they will lack full control because of the seamless boundaries across which information moves globally. Local dominance may be achieved temporarily, but dominance of global cyberspace will be impossible.

Threats from cyberspace. Cyberspace will continue to be contested out to 2035, by a larger and more diverse range of actors. The challenges to information and infrastructure security will be immense in 2035, with cyber attacks growing in scope, frequency and impact. Adversaries will be adaptive and be able to develop malicious cyber effects that strike at strategic, operational and tactical levels – not just against traditional military and critical infrastructure targets.

Computers and networks will continue to be compromised either by delivering malicious software to penetrate and damage information systems, or by corrupting the electronic component supply chain. This

may result in systems that do not function properly or securely and it may not even be evident that a cyber attack has occurred. We will also face the ongoing risk of insider access to stored sensitive information and the resulting threat of unauthorised sharing.

Cyber capabilities. Cyber capabilities will be integrated into overall targeting processes, contributing to a broad-based deterrent posture. Capabilities will become more prevalent and mainstream as they become better understood. Cyber activity may offer a credible way to provide deterrent effect that complies with the principle of distinction, perhaps by threatening a state's critical infrastructure, rendering that state open to coercion.⁴⁶ Effective deterrence through cyber activity will have to overcome a number of obstacles. These obstacles include ensuring that attacks can be directly attributed, and are not mistaken for the efforts of hactivists; making certain that attacks will always have the desired effect; and stopping the effects from being easily reversed.

Electromagnetic environment

The electromagnetic environment is defined as: the totality of electromagnetic phenomena existing at a given location.⁴⁷ The electromagnetic environment permeates the physical environment and overlaps with cyberspace as information passes through it. It is an integral part of the joint operating environment and its importance will increase further out to 2035. Defence's ability to communicate, navigate, deliver kinetic and non-kinetic effects, and gain situational awareness and understanding is dependent on access to the electromagnetic spectrum. Where bandwidth is limited, our access to the spectrum may be constrained by commercial operators seeking to expand

⁴⁶ Libicki, M. (2009), 'Cyberdeterrence and Cyberwar'.

⁴⁷ Allied Administrative Publication (AAP)-06, (2014), 'NATO Glossary of Terms and Definition'.



The volume of goods moving across the global commons is likely to increase dramatically

their own use. Increasing reliance on space-based technologies will increase our electromagnetic spectrum vulnerability.

Electronic warfare capabilities. By 2035, advanced electronic warfare capabilities will have become ubiquitous. As these capabilities proliferate, less capable adversaries will modify them, creating a broad range of electronic warfare threats. To survive, our information, systems and platforms will need electromagnetic protection to be resilient to electronic attack and able to operate in hostile electromagnetic environments. Electronic defence measures will need to continue to counter the threat from improvised explosive devices, as well as mitigate the effects of radio frequency, infrared or laser guided weapons. Passive and active protection measures will be required to defend our data-networks and systems from cyber attacks conducted through the electromagnetic environment. Countermeasures and mitigating electronic warfare attacks will be important, though reinvigorating and exploiting electronic attack capabilities could ensure Defence possesses operational advantage. However, Defence will also need to reduce its reliance on the electromagnetic spectrum.

Physical environment

This section considers some of the factors likely to characterise the physical environment in 2035. These are: the global commons as a key enabler of globalisation; sovereign territory remaining key to the international order; the increasing complexity and ambiguity of actors in the land environment; and the urban and littoral challenge. It does not include what some consider to be the 'virtual global commons' of cyberspace and the electromagnetic environment which have already been considered.

The importance of the global commons

The high seas, the air above it, and space constitute the physical global commons. To varying degrees, they are largely accessible by all actors and not subject to national jurisdiction – although they are all managed and controlled to some degree through international treaties and agreements. The global commons present opportunities to build partnerships to tackle shared problems out to 2035.



De-conflicting orbits will be a growing problem

Access and vulnerabilities. Maintaining UK access to the global commons will be essential for ensuring global reach, national prosperity and to deliver strategic effect. The global commons are enablers of globalisation and, out to 2035, will continue to facilitate ready access to the land and its people, principally through ports, airports and satellite-based communications. There are likely to be an increasing number of access points to the global commons by 2035, and direct transport routes will be more typical. The global commons will remain a critical enabler of international security, trade and communication, and will act increasingly as a conduit of military power.^{48,49} However, the global commons also contain inherent vulnerabilities, such

as strategic choke points, that adversaries and criminals may exploit. Greater access to the global commons will make the world increasingly interconnected, but also bring wide variations in security standards. Our security will only be as good as the weakest link in the chain, potentially resulting in enhanced risks from terrorism and the spread of infectious diseases.

Supply lines. There is currently an extremely high volume of goods moved across the global commons, and this is likely to increase dramatically out to 2035. Working with international partners, our Armed Forces will contribute to the continued flow of maritime trade and air movements around the globe.

There will be greater summer use of Arctic sea routes by 2035, in particular the Northern Sea Route, north of Russia. This will give Russia influence over the movement of trade, as sea routes to and from North-East Asia

48 Redden, M. E. and Hughes, M. P. (2010), 'Global Commons and Domain Interrelationships: Time for a New Conceptual Framework?.'

49 Brzezinski, Z. (2012), 'Strategic Vision: America and the Crisis of Global Power'.

will be shorter. If the UK develops significant trade dependencies, and if companies for which the UK has some responsibility use this route, access could become a security issue for the UK both at sea and in the air. Another aspect is greater use of the Eastern Atlantic and narrows such as the Dover Straits by commercial shipping. UK responsibilities for governance and secured access of these routes will need to be considered. In a more confrontational future, some states could continue to develop capabilities for sea and air control, although advances in technology may also enhance our own capabilities and access, depending on our ability to exploit them.

Dependency on space. Every part of the UK's critical national infrastructure relies to some extent on space capabilities, and this dependency will increase greatly out to 2035. However, our reliance on space is not always obvious to users – and in many cases the required capabilities are hosted by non-UK space service providers, increasing our national vulnerability. Access to space is already highly competitive in both orbital capacity and bandwidth: emerging space-faring nations, often with opposing interests, will increasingly seek equitable access to it. They are likely to contest the established order by disputing treaties and customary agreements and compete for the best satellite orbits.⁵⁰ De-conflicting orbits will be a growing problem, as will the proliferation of debris and collisions in space. Low-cost launch capabilities will make access to space easier, including for adversarial non-state actors and criminals. Space launches will either serve mass-market end-users such as satellite communications (demanding increased bandwidth) or provide bespoke services such as specialist geographic imagery.⁵¹ Military users of space will continue to rely on civilian companies

to operate space services and provide space vehicles and equipment.⁵² These companies may be as important to the UK in 2035 as the ship-building industry was in the 20th century.

Exclusive economic zones. The physical global commons allows access to exclusive economic zones, territorial waters and all littoral regions. In 2035, the most important maritime security challenge is likely to centre around exclusive economic zones.⁵³ They will be a focus for criminal activity as well as a source of friction between developed and developing states, particularly as states enforce their jurisdiction. As offshore energy cultivation increases,⁵⁴ these tensions are likely to intensify.

Governance. In 2035, shipping routes are likely to be increasingly contested amidst a range of rising sovereignty claims. This is likely to lead to increasing friction between those who insist on freedom of the high seas and navigation under the context of international waters (supported by international norms and convention) and those who do not.

While international airspace is subject to civil or military airspace control there is no agreement on how far airspace extends vertically towards space – although for practical purposes the limit is currently considered to be as high as aircraft can fly.

In 2035, the most important maritime security challenge is likely to centre around exclusive economic zones.

52 For example, Surrey Satellite Technology Laboratory provides and operates a military Intelligence Surveillance and Reconnaissance space capability for Nigeria.

53 The UK's exclusive economic zones came into force in April 2014 and is the world's fifth largest behind the US, France, Australia and Russia.

54 Offshore energy supplies will expand by 2035 – offshore oil production is expected to be 48% of world supply and natural gas will see a 60% increase. Offshore platforms will grow from 270 to over 600 over the next 20 years, with increases in the Arctic, Eastern Mediterranean, North Pacific, West Africa and South-East Asia. There will be at least 100 times as many wind farms as there are today by 2035, and tidal farms may reach 22,000.

50 UK Ministry of Defence, DCDC. (2013), 'JDP 0-30, Air and Space Doctrine'.

51 Reuters (2014), 'Global Spending on Space Falls, Emerging States are Spending More'.



Future urban operations will be hugely challenging

By 2035, technological advances will allow flight at ever-higher altitudes, blurring further the distinction between air and space. These technologies may stretch our ability to police international airspace and defend our sovereign territory from the air.

Ambiguity, differing interpretations and disagreements over norms of behaviours and governance on the use of the global commons, exclusive economic zones, international airspace and space may lead to confrontation.

Sovereign territory

Sovereign territory is characterised by the concentration of people and their daily pursuits on the land, in adjacent territorial waters and in the airspace above. Operating beyond the urban environment is likely to remain essential in 2035 and it will present armed forces with a range of diverse and challenging conditions: for example, arctic, desert, jungle, forest, riverine, coastal and mountainous.

In 2035, with the exception of Antarctica, all land masses are likely to remain declared and internationally recognised as sovereign under

the governance and authority of nation states, or other autonomous or *de facto* governance structures. However, tensions arising across the borders of some sovereign territories are likely to be more prevalent. Driven by the need for access to resources and subsequently exploiting and transporting them, the sovereignty of some lands is likely to become more directly contested. Changes as a result of climate change or intensified production methods are likely to increase the severity of such tensions. Commercial interests, driven by greater resource-scarcity, may also compete directly with national interests, leading to a blurring of the national instruments of power.

The complexity of actors in the land environment.

The land environment will be an increasingly complex tapestry of multiple actors with shifting or ambiguous allegiances. Some of our most likely adversaries (extremist non-state actors) can be expected to operate in informally governed spaces, seeking to gain freedom of manoeuvre and, ultimately, strategic advantage. They are unlikely to be able to operate across all environments freely or concurrently. Out to 2035 they will seek to identify and exploit our weaknesses, creating favourable conditions for themselves,

probably using novel technologies and cyberspace. Not all actors will be hostile, so identifying threats and opportunities will be vital. Whilst the physical terrain may be transformed as a result of climate change and urbanisation, it is amongst the human terrain where the most dynamic and radical change can be expected as a result of global trends. Defence will need to respond with a comprehensive understanding of this volatile and complex environment to shape it effectively.

The urban and littoral challenge

With increasing urbanisation, cities will be more physically, culturally and institutionally complex, with major cities the key hubs of human activity in 2035. At their best, future cities will be information-rich environments and centres for change, commerce, innovation and learning. Many will represent the pinnacle of human efficiency. Developed cities will be characterised by the latest high-tech transport systems, excellent medical facilities, thriving business sectors and modern, eco-friendly homes. Poorer urban areas, though, will be unable to keep up with the pace of growth and change, lacking the necessary resilience and infrastructure.

Physically, cities in 2035 will remain characterised by a diverse range of infrastructure, from the glass and concrete of a central business district to the tin shacks and open sewers of slums, perhaps just a short distance away. They will present a complex multi-dimensional challenge – containing the street level, roof tops, sewers and tunnels, riverine, surface, sub-surface, air, space, cyberspace and the electromagnetic environment.⁵⁵ The scale of the city challenge will be potentially overwhelming and every urban centre will be unique, requiring a bespoke understanding. All cities will be vulnerable to disease outbreak and transmission, particularly in densely-packed poorer areas. Most cities will contain ports and airports – essential for access, trade

and globalisation. The effects of climate change will be most keenly felt in densely populated coastal cities, leading to instability and suffering.

For our Armed Forces, the urban environment will be one of the most challenging areas to operate in. The city, and its surrounds, will become an increasingly complex and ambiguous tapestry of multiple actors with shifting allegiances, in which we may be required to operate in a variety of ways, from major conflict at range to peace support and humanitarian operations.

Where cities are located on the littoral – a complex operating environment in its own right – the complexities of the urban environment will be amplified and even more dynamic. This will exacerbate further the operating challenges.

Future legal aspects

Human rights law. Out to 2035, our Armed Forces are likely to be increasingly constrained by both national and international human rights legislation. The precise understanding and applicability of the Law of Armed Conflict may present challenges in keeping pace with technological developments, such as wider use of more sophisticated automated systems. ‘Soft’ laws, such as UN General Assembly Resolutions and temporary international agreements, are likely to become more prevalent as a result. In general, the UK should expect greater domestic and international legal scrutiny and criticism of military operations out to 2035, both informed and ill-informed.

Lawfare and technology. ‘Lawfare’ – the strategy of using law, rather than traditional means, to achieve an operational objective – is likely to be used more prominently by 2035. The UK may employ lawfare itself, and we will also need to understand how an adversary may use the law against us. For example, adversaries may sponsor legal actions as a way of challenging our Armed Forces using the legal process.

⁵⁵ Dr Kilcullen, D. (2014), ‘Urbanisation: A briefing to DCDC’.

Chapter 2 – Key points

Actors

- In 2035 there is likely to be growing competition between states for access to, and influence over, ever-scarcer resources.
- Traditional state-on-state conflict cannot be ruled out over the next 20 years, but state-sponsored terror attacks, use of proxies and cyber attacks are more likely.
- Three-way engagement between militaries, non-governmental organisations and multinational corporations will become increasingly important out to 2035. For urban operations, engagement with city authorities will be particularly relevant.
- Extremist non-state actors will be more able to exploit a wider array of military capabilities, using innovative tactics that exploit our inherent vulnerabilities, including any institutional inertia. They are likely to develop ever-higher levels of lethality to counter our protection systems and may even have access to weapons of mass effect.

Institutions

- For the UK, NATO will remain the defence alliance of choice – providing the continued commitment to Article 5 but also the means of interoperability with a wide range of nations that could form coalitions of the willing.
- In 2035, the UN is likely to work through regional organisations to achieve its aims, including a greater role in upstream conflict prevention. The need for large-scale UN operations – perhaps in Africa – and the UK's involvement in (and possible leadership of) them should not be discounted.

Culture and identity

- The growth and proliferation of social media is likely to create new forms of identity-based 'turbulence' or volatility, which gain strength by their associations. This is likely to intensify and complicate battlespaces by broadening audiences and energising 'causes' for which people fight, making pragmatic compromise harder to accept.
- Social media's readily-available open-source intelligence-gathering advantages are likely to be used for control, manipulation and targeting.
- Faith-based ideologies will continue to shape many conflicts around the world in 2035.
- Tensions arising from differences of nationality and culture and a rise in 'identity politics' will carry a high risk of sectarian or communal violence.
- Analysis and predictive modelling of social behaviour will increasingly support operations.

Technology

- The UK and other Western militaries, probably with the exception of the US, will almost certainly have been overtaken in some technologies by 2035, and may need to become accustomed to being overmatched by derived military capabilities.
- By 2035, a diverse range of actors will be able to access capabilities once restricted to just a few states. Illicit and unregulated technology transfer will exacerbate the threat to the UK.
- Technological change will accelerate, serving to highlight inadequacies in less adaptable procurement processes within Defence.
- By 2035, proliferation will enable a wider range of our potential adversaries to deploy weapons to deny our access to, and freedom of movement within, operational areas. The aim of our adversaries is likely to be to deter Western powers by raising the potential cost of action.
- Automated systems, including those that are armed, will proliferate over the next 20 years. Advances in technology will almost certainly enable swarm attacks, allowing numerous devices to act in concert. This may serve to counter the advantage of high-end systems.
- Additive manufacturing may make our logistics chain lighter. This will be key to operating in non-permissive environments, especially when the support chain is long, expensive or threatened. It may also allow individuals, non-state actors and developing states the capability to produce very large numbers of cheap, precision weapons.
- By 2035, physical and cognitive performance will be artificially enhanced via biomechanical systems such as exo-skeletons or prosthetics, wearable devices and sensors, and memory-enhancing drugs.
- Synthetic biological components may lead to new pathogens being deliberately or accidentally created and released, potentially causing or exacerbating pandemics. By 2035, it may even be possible to create genetic weapons.
- Defence will need to understand the impact on privacy, assurance, jurisdiction and security for data stored on any foreign based servers. Such data servers will become an important part of critical national infrastructure, but may not have the type of protection afforded by UK sovereignty.
- By 2035, persistent real-time, multi-sensor surveillance capabilities will be ubiquitous, cheap and passive, offering considerable advantage to a range of actors. This will have significant implications for operational security.

Cyberspace

- Cyberspace will be ubiquitous by 2035, pervading every aspect of the physical environments to a far higher degree than today.
- Dominance of global cyberspace will be impossible: states will struggle to control cyberspace, because its infrastructure is so widely dispersed.
- Cyber activity may offer a credible way to provide deterrent effect that complies with the principle of distinction, perhaps by threatening a state's critical infrastructure, rendering that state open to coercion.

Electromagnetic environment

- Advanced electronic warfare capabilities will be ubiquitous and proliferate to less capable adversaries, creating a broad range of electronic warfare threats.
- Countermeasures and mitigation to electronic warfare attack will be important. Reinvigorating and exploiting attack capabilities could ensure Defence possesses operational advantage.

Physical environment

- Maintaining UK access to the global commons will be essential for ensuring global reach, national prosperity and to deliver strategic effect.
- Increasing reliance on space-based technologies will increase our electromagnetic spectrum vulnerability, partly because enabling capabilities are often hosted by non-UK space service providers. Every part of the UK's critical national infrastructure relies to some extent on space capabilities, and this dependency will increase greatly out to 2035.
- Technological advances, by 2035, will allow flight at ever-higher altitudes, blurring further the distinction between air and space. These technologies may stretch our ability to police international airspace and defend our sovereign territory from the air.
- For our Armed Forces, the urban environment will be one of the most challenging areas in which to operate. Cities will be complex and multi-dimensional. Armed forces operating in future cities will have to consider aspects of the environment as diverse as subterranean spaces and cyberspace. The scale of this challenge will be potentially overwhelming and every urban centre will be unique, requiring a bespoke understanding.
- The effects of climate change will be most keenly felt in densely populated coastal cities, leading to instability and suffering.
- Where cities are located on the littoral, the inherent complexities of the urban operating environment will be amplified.

Future legal aspects

- The precise understanding and applicability of the Law of Armed Conflict may present challenges in keeping pace with technological developments, such as wider use of more sophisticated automated systems.



Chapter 3

Implications for Defence

Introduction. FOE 35 presents a challenging picture of the operating environment in 20 years time, but there is much Defence can do to prepare for the future. Acknowledging that we will be vulnerable to a growing range of threats is essential. We can then take decisions to mitigate these vulnerabilities – developing ways and means that will give us a better chance of safeguarding our interests.

Based on the analysis in Chapters 1 and 2, the most significant implications for Defence in 2035 concern:

- the increased and vital importance of the ‘understand’ function;
- technology and the utility of remote and automated systems;
- the need to overcome anti-access and area denial capabilities;
- the urban and littoral challenge;
- the blurring of UK mainland and overseas threats;

- the increased likelihood of military support for humanitarian assistance and disaster relief;
- the importance of maintaining the ability to reconstitute capability; and
- agility.

These implications are likely to have significant consequences for future force development and are illustrated in the diagram on page 30.

The challenge

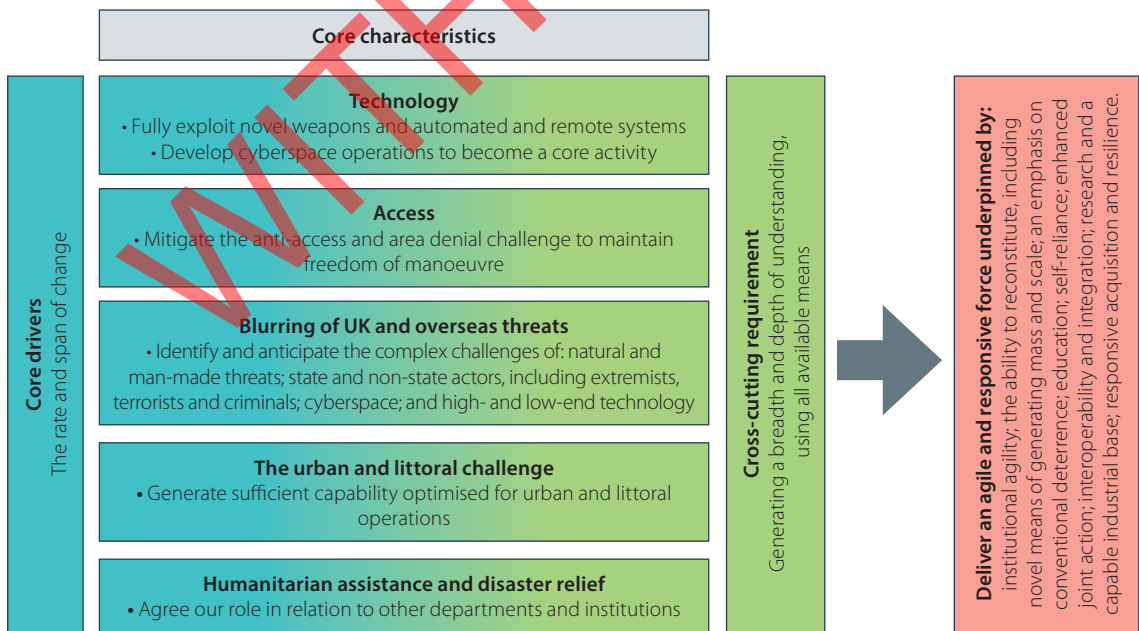
Chapter 1 highlighted that Defence will provide enduring support to the UK’s *National Security Strategy* by **protecting** the UK mainland, our Overseas Territories and citizens abroad; **shaping** the international environment through proactive global engagement and capacity building; and **responding** to crises by projecting military power. The characteristics of the future operating environment described in

Chapter 2 indicate both significant threats and opportunities for Defence. On the basis of that analysis, FOE 35 suggests that our immediate priorities should be: developing the required capability to generate and improve levels of understanding; a focus on the defence of the UK mainland; and investment in emerging technologies, especially automated systems. To underpin conventional deterrence, for enduring campaigns and in mitigation of existential threats, Defence must also focus on reconstitution. Specifically, those capabilities that underpin the creation of greater force elements, particularly when the level of response required exceeds our ability to do so with the core force. Thereafter, as we move into 2035, we will need to exploit our new levels of understanding and develop capabilities to meet a spectrum of challenges, from humanitarian aid operations to overcoming complex anti-access and area denial threats, and operations in evermore challenging urban environments.

The increased importance of the ‘understand’ function

Generating understanding. Achieving a nuanced understanding of the operating environment will be more challenging – and more important – out to 2035. Defence’s capacity to collect and process useful intelligence lawfully from amongst a vast and growing volume of information will be a key technical challenge over the next 20 years. It may be able to meet at least part of that challenge by using the sophisticated techniques of Big Data analytics.

Although technology developments will offer opportunities, they will not provide the whole answer to the problems of the future operating environment. Indeed, an over reliance on technical solutions may undermine the ability of our personnel to learn from, and adapt to, the challenges they face and then exploit them to our advantage. We will need to possess greater



Implications for Defence

awareness of local and regional politics, law, human persuasion, behaviour and culture, supplemented by a broad range of experiences. Opportunities for overseas engagement, further education and cultural immersion will be just some of the ways this can be achieved. Our diasporas will provide a crucial source of knowledge. As a priority, Defence should access them through recruiting and engagement opportunities. Defence needs to acknowledge that building the required level of understanding takes time and this will have to occur in a highly competitive and volatile space. This will require genuine investment and, hence, traditional attitudes towards career timelines and promotion are unlikely to be adequate.

Defence's ability to share understanding, and be informed by others, will make it easier to operate in areas and regions that are outside our own experiences, greatly enhancing our future utility. To do this we will need to change our ethos and behaviour, which may often be at odds with our current requirements for operations security and secrecy. The understanding that Defence generates must be shared as widely as possible, not only across UK Government, but also between our key allies and partners, with whom we will need to develop more expansive sharing protocols.

Better understanding and intelligence, if exploited, will allow us to operate with greater precision at the operational and strategic level. It will also allow our senior decision-makers to offer better military advice and more informed options. An increased level of understanding will enable more informed and effective employment of our Armed Forces. It will also be fundamental in underpinning conventional and nuclear deterrence as well as coercion. Coercion will become increasingly important in the face of emerging threats from state and non-state actors. But this must come with some caveats – our understanding and intelligence will always be imperfect. Others, including potential adversaries, will be competing in the same single information environment, and may use ambiguous means

to mask their true intentions, motivations or threats they pose.

Understanding our own vulnerabilities.

A nuanced understanding of the operating environment will need to include a full understanding of our own vulnerabilities. With the blurring of the overseas and mainland threats, and the pervasive nature of cyber and space, the UK's critical national and military infrastructure will become increasingly vulnerable; Defence must identify and mitigate against such associated risks.

Remote and automated systems

The proliferation of automated systems, and their use by a variety of actors, will spawn a diverse range of applications across all environments in 2035. In some applications their utility will be optimised through augmenting human activity, while other applications may drive the replacement of humans. Their increased use in combat and support functions will reduce the risk to

“The proliferation of automated systems and their use by a variety of actors will spawn a diverse range of applications across all environments in 2035.”



Optimising the human/machine interface...

//
Defence will need to be able to overcome the challenges posed by anti-access and area denial, possibly fighting to gain access to the global commons...

military personnel and thereby potentially change the threshold for the use of force. Fewer casualties may lower political risk and any public reticence for a military response, as could an increase in precision targeting – which may reduce the impact on civilians. Automated systems offer almost unlimited potential, yet using them is likely to be more constrained by legal and ethical concerns than by the limits of the technology itself. However, some actors may not be bound by such concerns, potentially developing combat systems that may target people indiscriminately.

Automated combat systems are likely to be developed along two different paths: high-end, multi-role, exquisite capabilities that seek to emulate and potentially replace high-end manned systems; and low-end systems that are highly specialised and limited to one or two missions. High-end systems could be more challenging to develop (and more expensive to procure and operate) than manned systems. Conversely, low-end systems may be better able to rapidly exploit technology to fulfil new and specific operational requirements. Defence will need to make exploiting emerging technology and capability in automated systems a priority, as well as countering our opponents' systems.

Access, anti-access and area denial

The proliferation of weapons technology will mean that many future adversaries will have capabilities designed to prevent our access to the maritime, land, air, space, cyberspace and electromagnetic environments. Defence will need to be able to overcome the challenges posed by anti-access and area denial, possibly fighting to gain access to the global commons before further action can take place. The range and survivability of our systems and bases will become a critical factor. Investment in niche capabilities that exploit weakness in anti-access and area denial systems will be required. Mitigating the risks associated with these capabilities will be essential if we are to maintain our

freedom of manoeuvre and action, and our options for projecting power in response to crises.

The urban and littoral challenge

Projecting military power into an urban environment (whether it is from maritime, land, air, cyberspace or the electromagnetic spectrum) will remain fraught with difficulties, particularly in the littoral. We may need novel ways and means to overcome them.

A range of state and non-state actors may deny our freedom to operate in highly congested environments. The scale of civil maritime, air, land and information traffic in 2035 is likely to be significant, especially if we require access to commercial ports, airports and communication nodes from which to mount further operations. The competition for freedom to base, operate and manoeuvre will be more challenging than today, as will the challenges and consequences of operating in future cities.

This may require us to conduct more of our activity remotely, or from a stand-off location, so that we do not become embroiled in lengthy and intensive urban operations. On occasion, however, we may have no choice but to operate in an urban area. This will be particularly true if our Armed Forces are called upon to conduct a non-combatant evacuation operation, hostage rescue or support a humanitarian operation within a city.

Blurring of UK and overseas threats

Out to 2035, the UK mainland may need to be defended from a broad range of natural and man-made threats, especially as those threats blur between state and non-state actors. Threats from terrorism will remain and may become more severe as our adversaries exploit greater connectivity.



Our Armed Forces will still be expected to support humanitarian assistance and disaster relief operations

The continuing drive to perform a 'spectacular' attack, enabled by increased proliferation, may mean the threat from weaponised chemical, biological, radiological or possibly nuclear agents will endure and could increase. However, due to the inherent difficulty in conducting a mass casualty attack involving chemical, biological, radiological or even nuclear weapons, future terrorist attacks are more likely to be low-tech and well-coordinated, perhaps including small arms and conventional explosive devices. However, in 2035 we will need to be mindful of empowered and well-resourced terrorists able to exploit the potential offered by sophisticated technology.

Given the ubiquitous and pervasive nature of cyberspace in 2035, threats will come from a range of actors, targeting intellectual property as well as critical national infrastructure, such as data servers. Countering the growing cyber threat will be critical to safeguarding economic prosperity and national security. Government and industry will need to

develop adaptable countermeasures and situational awareness. Appropriately targeted recruitment, education, training and retention of personnel for cyber operations will be key, acknowledging that this will be a mainstream activity.

Humanitarian assistance and disaster relief

The UK will be affected by more severe and frequent weather events as a result of climate change. Such events could overwhelm local resources, necessitating military support. There will be an enduring need for our Armed Forces to provide niche capabilities such as logistics and engineering capabilities across all three Services. Defence may also be required to generate a ready supply of manpower or use war-fighting equipment in novel ways to aid the civilian population.

More intense, frequent and longer extreme climatic events will not only affect the UK out to 2035. Humanitarian disasters across the world will increasingly result from climate

“
...humanitarian
assistance and
disaster relief
operations
may become
more common
in 2035...”
”

change. Our Armed Forces, especially if forward deployed, could be expected to assist our allies and partners, most probably in support of other UK Government departments and non-governmental organisations. This assistance is likely to take the form of providing security, access, lift and niche capabilities. Consequently, humanitarian assistance and disaster relief operations may become more common in 2035 than they are today.

Reconstitution

It is possible that there may be future state-on-state conflicts in which the UK could be involved. In the event that an unexpected existential threat emerges, our Armed Forces must have sufficient resilience within their structures, processes and capabilities to be able to reconstitute additional forces. Regeneration of capability by using Reserve forces will be important, but we also need to be able to grow additional forces to create sustained resilience. The key elements of being able to reconstitute will be:

- sufficient ‘seed corn’ expertise, capable of organising, training and educating new and reserve units;
- enough real estate, platforms and logistics to train the required personnel and units on time;
- access to sufficient industrial capacity;
- good links to industry, with an urgent operational requirement purchasing system that can provide additional platforms and equipment quickly (off-the-shelf where necessary);
- the command and control structure to lead and direct reconstitution; and, where possible,
- a national early warning system that can give us sufficient notice to take the decision to reconstitute.

Generating mass effect and scale. In a state-on-state conflict or in an enduring campaign, Defence may still need to deliver

mass effect and scale of effort in areas where our Armed Forces have potential deficits. Reconstitution is one avenue of potentially achieving this, provided all key elements are available. Others include: leveraging the capabilities of our allies, particularly where our interests coincide; and technological solutions, such as using large quantities of low-cost automated systems. Mass effect can also be delivered in cyberspace. In the timeframe of 2035, Defence may need a combination of all these.

Agility

Key to future success is agility, which comprises adaptability and flexibility in both capability and approach, and specifically in terms of our thinking. To adapt is to adjust to new conditions and the ability to do this quicker than our adversaries has always been important. Defence will need to become a more effective learning organisation: adjusting, responding and exploiting quickly in the face of a wider range of threats in an increasingly volatile environment. Adaption will be vital at all levels and in all activities to overcome the rapidly developing and varied technological, physical, cultural and institutional challenges we will face in 2035.

Human capability. Military strength has traditionally been expressed in terms of equipment and uniformed personnel numbers.⁵⁶ Increasingly, military strength will be expressed in terms of human capability across the Whole Force, and establishing the right mix of regulars, reserves, civilians and contractors will be critical. ‘Generation Alpha’ – the young children of today who will become the potential recruits of 2035 – are likely to seek a portfolio approach to career development. As our most important asset becomes harder to recruit and retain in the future, Defence will need to access

⁵⁶ Publishers such as International Institute of Strategic Studies and Janes publish annual assessments of military strength, with detailed numerical statistics of equipment and personnel, for example, the International Institute of Strategic Studies ‘The Military Balance’.



The need to operate in austere environments will endure

the human potential they offer to maintain our capability advantage. We will have to compete in a global employment market where competition for talent is likely to be high. Having been recruited and received training, our personnel will require an agile mind to face the challenges ahead.

Young people will be increasingly 'tech savvy' as users, but they may lack the know-how required to master the technical skills to engineer or programme systems. The training requirements to keep pace with technology will be considerable. In particular, the critical role of networks and exploiting the information they bear will be a major challenge: it will require human innovation, not just technological ones. Our challenge will be to recruit and develop people who are comfortable with change and can adapt as necessary.

Education. Defence needs to become a better learning organisation that can quickly adapt at the strategic level. At the operational level, Defence must rapidly and

flexibly meet novel threats with suitably structured, trained and ready forces. The ability to adapt at the tactical level will require highly trained, educated and motivated Service personnel with a range of equipment and technology optimised for the varied missions we may be asked to deliver.

Operating in austere environments.

Our ability to operate in more austere environments will remain essential in 2035. Violent conflict and natural disasters will continue to test the infrastructure and services many take for granted, in some cases reducing the capacity of a host-nation to support deployed operations. Maximising our ability to be self-reliant, for what may be extended periods of time, will be critical. Fully exploiting our overseas bases and sea-basing, partnerships and alliances will be an essential part of managing these sustainment and austerity challenges, to gain and maintain theatre access. Technological solutions, particularly automation, additive

“
By 2035,
increased
global
connectivity
will mean
that any
unintended
consequences
of our joint
actions may
be more
far-reaching
and
damaging
than
previously
envisaged.
”



Credit: Aircraft Carrier Alliance

Projecting military power out to 2035 and beyond

manufacturing and efficient forms of propulsion and power generation will also play a key role, as will the robustness of our people and equipment.

Enhancing joint action. Joint action is executed across all environments to affect the capabilities and understanding of our adversaries, allowing us to impact their decision-making. Deterrence and coercion are key current examples of such action, but fully exploiting cyberspace and the electromagnetic spectrum will be increasingly vital in pursuit of effective joint action in 2035. Our access and freedom of action within them will be critical to operational success and overcoming anti-access and area denial. Similarly our adversaries are likely to increase their use of non-lethal methods across the whole spectrum of joint activity (from direct attacks to psychological operations), affecting our own perceptions of the operating environment and our behaviours within it. Any mistakes we make are likely to be ruthlessly exploited.

To enhance the potential of joint action, we must train together, exchange personnel

more often and exploit collective efficiencies. Exchanging personnel should not be limited to exchanges between the Services but more broadly; with the Diplomatic Service, other UK Government departments and even with the private sector. The flexibility innate in military command structures should be used more progressively, empowering commanders to develop their people in innovative ways within the context of the Joint Force.

By 2035, increased global connectivity will mean that any unintended consequences of our joint actions may be more far-reaching and damaging than previously envisaged. Conversely, there will be positive unintended consequences and we must have the agility to exploit these to the fullest extent across the whole joint spectrum, through both decentralised execution and mission command.

Interoperability and integration. In a multipolar world, future alliances and partnerships are likely to be more dynamic. New threats and crises will emerge quickly, often requiring the intervention of departments across UK Government,

working with civil society. Existing alliances and partnerships will remain important, particularly NATO, but more *ad hoc* coalitions consisting of new partners, are likely to emerge to tackle specific crises. In 2035, we will be presented with a more diverse and blurred mosaic of state and non-state actors, including non-governmental organisations, large multinational corporations and private security contractors. With more states capable of intervention, more state agencies will be involved in future crises. In these circumstances, our ability to integrate and be interoperable with *ad hoc* coalitions and partnerships, spanning a range of technological capabilities and actors, will be a key factor in success. UK Defence may be called upon to take part in, or lead, such arrangements.

Greater emphasis on conventional deterrence. Defence's primary tasks include deterring, containing and defeating threats to the UK, its Overseas Territories, citizens and interests. A key part of this deterrence is our ability to project power using conventional means. Our people, force structures and capabilities must be both credible and capable of delivering this conventional deterrence at the right time and place; this capability must also be communicated. With a more diverse range of actors and threats, deterrence will become increasingly complicated. We must therefore be capable of meeting the most likely conventional and unconventional threats, with forces balanced accordingly. By 2035, this may not look like the balanced force of today – but we must be agile enough to evolve.

Research and industrial base. Knowledge of technology will not be geographically distributed evenly in 2035. The last few decades have seen rapid military de-industrialisation of the UK. Our reliance on foreign suppliers and strategic, political and industrial partnerships has reduced our independence.

Defence will need to track future technologies that may offer new capabilities or pose threats. Instilling a culture that

focuses on looking for opportunities in technology and simultaneously seeking to reduce the cost of delivering capabilities will be important. Defence will need to balance current programmes with long-term speculative research which may deliver no immediate exploitation.⁵⁷ Technological horizon scanning may help us to understand the changing context for future operations and trends in technology development. Risk will require to be mitigated in those areas where we choose not to invest, or to invest less, by leveraging investment and influence with our allies and partners. A coordinated (burden sharing) approach with allies may also allow broader harnessing of new technologies and capabilities. Similarly, Defence will also need to forge strong links with relevant civil areas of expertise.

We are likely to use this knowledge to shape our future capabilities. For example, by 2035, fuel cells are likely to be cheap, lightweight and compact (even wearable). Non-contact power transfer to personnel, remote sensors or platforms will be widespread. Bio-fuels could be available from locally-grown materials or extracted from waste products. Solar power generated from rucksack-sized collapsible panels could recharge small devices.

Wearable devices with multiple sensors or biological markers could augment sensory data through new human-sensor interfaces (Google Glass is a present-day example). High-energy lasers may provide air defence and possibly anti-satellite roles; precise non-lethal engagement will also be possible. Radio frequency weapons will also have the potential for persistent disruption or damage to electronically sophisticated equipment. Advanced sensors will detect difficult targets (camouflaged, under foliage or in a cluttered urban environment) or distinguish decoys, and be adaptive for all-weather or degraded atmospheric conditions.

The UK will require access to, and an understanding of, global science and

With a more diverse range of actors and threats, deterrence will become increasingly complicated.

⁵⁷ UK Ministry of Defence. (2012), 'National Security Through Technology: Technology, Equipment and Support for UK Defence and Security'.

//
In 2035
long-term
equipment
plans may
no longer be
viable...
//



technology information to inform national strategies, educate people technically and develop our industry. The skills and strengths of the UK science and technology community will play a greater role in the Whole Force concept. Delivering basic and technical skills, in particular resource availability and cost, will continue to cause challenges. We may also need to review inadvertent education of potential competitors.

Radical reform of our acquisition process.

In 2035, long-term equipment plans – with 10 to 20 year development programmes for 30 to 50 year life cycles – may no longer be viable given the rate at which future threats will evolve. Defence must be prepared to tailor and adapt its forces for each campaign, using new acquisition models where required. This may also involve adapting and modifying existing equipment and its current use in novel ways. Understanding and intelligence will be vital to provide sufficient warning time as threats emerge or evolve. Defence will also need to be better able to understand and exploit the potential of emerging civil and defence technologies, with agile and adaptive continuous development of capabilities. It will be critical that capabilities respond to military operational need and are supported by a modern and competitive defence industrial base.

Future models for acquisition will require collaboration between Defence, programme managers, platform builders and a wide customer base to reduce development costs, mitigate programme risks and share expertise. Effectively exploiting 'system-houses' (organisations that blend technologies and ideas to create new concepts) will offer advantages and efficiencies. 'Plug and play' architectures that enable rapid modular upgrades will allow an improved response to new threats and mitigate the risk of obsolescence with long-term equipment plans. A second, parallel, highly responsive and adaptable acquisition process that deters potential non-peer adversaries will be needed to contend with sudden and unexpected events. This will also serve to generate new capabilities and greater capacity more quickly, outside the core equipment programme – even though such capabilities may only be required for a specific purpose.

Pursuing niche technological dominance will need to be constantly assessed and balanced against cheap, often commercial, low-tech systems that provide effective, and sometimes asymmetric, capability. Constrained budgets will demand that Defence balances the cost of current capability against a range of possible new threats. Again, this will require a highly agile procurement process.

Establishing resilience. Ensuring system and infrastructure resilience against disruption, and retaining sufficient reversionary modes, will be critical out to 2035. Technological disruption is likely to have an increasing impact on space and cyberspace services and infrastructure. Cyber resilience could be improved by developing greater shared awareness of threats across Government, industry and allies. Ascertaining the UK's dependence, interdependence and co-dependence will be necessary to understand our true vulnerability. Defence is likely to increasingly rely on commercial off-the-shelf systems, which must be protected from disruption and meet military hardening standards. Resilience will be delivered by more than just technology. Regular combined exercises could test and improve systems and infrastructure, and ensure that we train in reversionary modes.

Conclusion

With rising equipment and personnel costs there will be difficult choices for Defence over the next 20 years. The UK will still need the military capabilities to act unilaterally to **protect** the mainland and Overseas Territories. The range of threats to the UK mainland are likely to be far more diverse and ambiguous than today from traditional threats such as chemical, biological, radiological and nuclear, ballistic missile attack and natural disasters to hacktivists and offensive cyber. This indicates a continuing – and potentially increasing – role for Defence in assisting civil authorities to ensure the safety of the UK population and protect critical national infrastructure. We will also need to retain our ability to evacuate UK personnel from overseas, which *in extremis* is still likely to require military means.

The future calls for a far greater understanding of the potential operating environment. Understanding goes beyond gaining intelligence – and the military will have a role in developing that understanding, through both traditional means such as human intelligence, as well



Generating mass in the future?

as lawfully exploiting new technologies such as Big Data analytics. Understanding will also underpin both conventional and nuclear deterrence. Attaining this level of understanding, partly through proactive forward engagement and peacetime military posture, will support the UK's efforts to **shape** the international environment and support the UK's wider prosperity. But we must also apply and exploit this understanding.

Along with deterrence and forward engagement, the UK will need the capability to **respond** to events and project power overseas to **protect** UK interests – either alone or with allies. These operations could be described as 'forward defence' – because they aim to prevent escalation and reduce, or eliminate, the threat to the UK or our interests. In the future operating environment these responses will be more challenging. The proliferation of technology

and advanced weapons systems will provide many more states with effective anti-access and area denial capabilities that will impact on operations in every environment. Defence will need to be able to mitigate these risks and overcome defence systems to deliver the required effects. This will call for the innovative use of cyber, precision and stand-off weapons, as well as stealth, layered defence and automated systems – across land, sea, air and cyberspace. These capabilities are likely to offer significant utility in attritional circumstances. Flexible joint logistic hubs (including the use of forward bases and sea basing) – may reduce the vulnerability

of support infrastructure and maintain our freedom of action. These flexible logistic hubs will allow us to operate across a range of activities, from conflict to humanitarian and peace support operations.

Finally, the UK will need to consider how it might reconstitute sufficient capability, for example, to conduct state-on-state conflict alongside its coalition partners. Maintaining command and control, and niche capabilities, including joint enablers, supported by an adaptable and flexible industrial base and conceptual development, will be key.

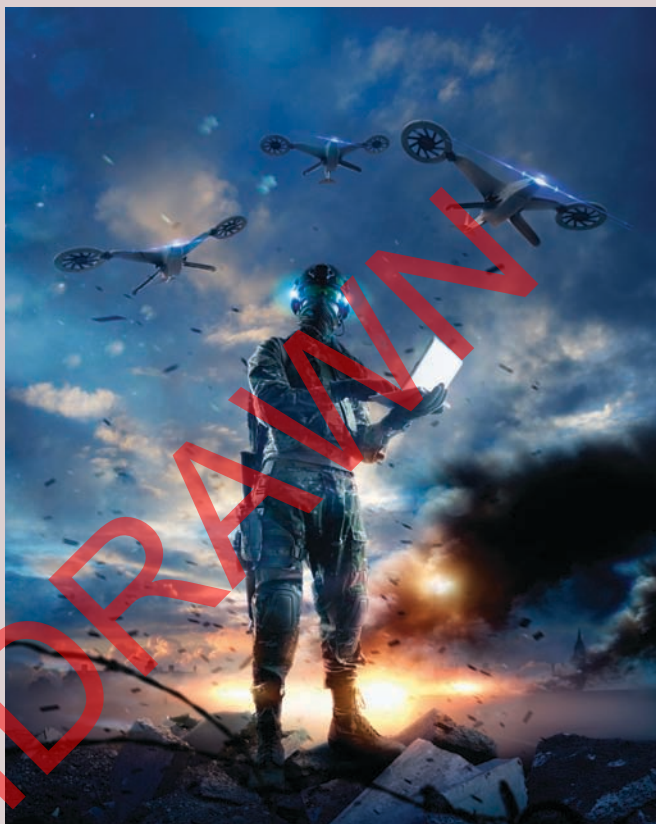
Chapter 3 – Key points

- The proliferation of military technology amongst potential adversaries means that our key systems may be vulnerable to technical exploitation or capability overmatch.
- Understanding will be fundamental in underpinning conventional and nuclear deterrence as well as coercion.
- The UK mainland will face a broad range of natural and man-made threats. It will be increasingly difficult to distinguish between threats from state and non-state actors.
- In the unlikely event that an existential threat to the UK emerges, mechanisms will need to be in place to provide warning and rapidly reconstitute sufficient forces to respond.
- Achieving a nuanced understanding of the operating environment will be more challenging – and more important – out to 2035.
- Future systems must be able to operate and survive, at range, against more sophisticated anti-access and area denial capabilities.
- Interoperability and adaptability will be crucial as bespoke alliances and partnerships become more important, both between nations and with non-state actors.
- Very long-term, inflexible procurement processes will no longer be sustainable.
- Increasingly, military strength will be expressed in terms of human capability across the Whole Force, and establishing the right mix of regulars, reserves, civilians and contractors will be critical.

A commander's perspective: 2035

The operational commander in 2035 will need to be as focused on cyber as on traditional environmental factors; it will be a mainstream element of joint and 'combined arms' operations. A rebalancing of our environmental focus and capabilities over the next 20 years may be needed because operational activity in 2035 will differ. It will be more varied because threats in the future are likely to come from a greater variety of sources: some novel and some more potent in relation to the actor's status. Some threats will be more complex and ambiguous, whilst others may still emanate from the barrel of the AK-47. Attacks may be launched by civilians, such as hactivists concealed in cities far from an operational theatre who may seek to disrupt ongoing operations or attack critical national infrastructure, perhaps out of pure mischief. Swarm attacks could be more prevalent, launched in the physical environment through a combination of mass, low technology and automated systems, demanding a response to deal with the high number of targets presented. But in the virtual environment, swarm attacks could be planned through crowd-sourcing before being executed through multiple access points in multiple countries, making deterrence and defence against them almost impossible. These could be orchestrated by terrorists, who could equally draw upon conventional legacy equipment, additive printed weaponry or perhaps weapons of mass effect. Attacks may also come in the form of increasingly highly automated systems or ballistic missiles.

Yet more of these threats may come increasingly in the form of a seemingly unethical, unconstrained 'collective of adversaries'. Such 'collectives' are likely to morph over time, attracting allegiance of a transactional nature from all manner of actors, from states to hactivists, armed with an array of varying capabilities and intentions. These actors are likely to have their own networks, which will be greater in size and capability than is feasible today, and



they are likely to be able to exploit porous borders more readily. So, the operational commander must seek even more clarity on potential threats because of the increased complexity and ambiguity of the future operational environment. The commander may, for example, be required to monitor social media in real time to judge social and human dynamics, observe emerging threats and even gauge and harness local public support for a mission. Our understanding of environments and actors must be sufficient to ensure we can protect, engage, coerce, deter (including by conventional means) and project military power, given the broader array of potential adversaries and the complexity of environments in 2035. The as yet unfathomed depths of cyberspace will be among those areas that require further exploration, as a place where adversaries

may loiter – it will be of national importance to ensure a response to a camouflaged cyber attack is directed at the actual perpetrator. Big Data analytics, with its accompanying opportunities and challenges, may help the commander pursue understanding, to overcome the risk of information overload. Increasingly powerful computers could improve the ability to forecast and perhaps provide courses of action for the operational commander – a capability that the adversary might also enjoy.

While traditionally the operational commander has focused on a single operational theatre, with the blurring of mainland and overseas threats, attention is likely to be diverted to the UK mainland because of the implications of operations abroad. Irrespective, the mainland, which will be more culturally complex, is likely to be more vulnerable over the next 20 years. Threats could range from a cyber attack (citizens may, through their own personal misfortune, recognise the need to be more self-disciplined in cyberspace and may demand inbuilt defences in electronic devices in the future) to a hostile non-state actor's unmanned aerial vehicle over a major city, perhaps targeting a VIP. If an attack comes in the form of ballistic missiles, will we know in advance what type of warhead is being projected by the missile? If not, how does the UK appropriately escalate or respond with force, or is defence the best approach? The deployed operational commander may have to have an increasing eye on mainland events, while drawing upon the knowledge of diaspora to assist understanding of a foreign nationality or culture.

With less time to respond to events due to a world increasingly interconnected, including by social media, the risk of a miscalculated military response is heightened. A comprehensive understanding will be paramount to help mitigate this risk, aided by forward engagement and exploitation of the vast quantities of all-source information likely to be available in 2035. Of course, any engagement by the military, even low level and benign in design, could be the

catalyst for more rapidly changing events. To contend with such dynamism, which will typify theatres increasingly due to the rate of change of technology, a more increasingly agile, perhaps radical approach, may be required to policy-making to enable commanders to pursue policy ends effectively. The risk is that law and policy, alongside ethical and moral considerations, might lag behind thereby constraining the employment of cutting-edge technology. And yet, with the increased proliferation of technology and information, some adversaries will have the scope to be increasingly agile and potent, perhaps without the legal and moral constraints that we are likely to face. The operational commander may seek to hold more operational risk to attain their goals. Yet technology trends will only serve to increase the potential for the compression of strategic to tactical levels. The commander may also seek increased use of automated platforms and weapon systems to create effects: perhaps to create those effects previously only attainable through 'mass', whilst minimising the risk of friendly casualties and those of innocents through exploitation of evermore precise weaponry.

In facing future threats and adversaries, particularly the 'collective of adversaries', the employment of strategic communications will need to be increasingly agile and more effectively targeted to contend with such an array. Even within such 'collectives', motivations and incentives may differ as they might within an alliance or partnership. The operational commander must strive to identify these so actors can be influenced. They will therefore require the very latest education and training to prevail in the complexity and ambiguity of the future operating environment, particularly so that emerging technologies can be employed optimally.

The operational commander will require force elements to be increasingly resilient, adaptable and agile. Our mindset must support this, and our own forces might need to be restructured more frequently

to allow opportunities to be seized. Componency might hinder the execution of operations. But flatter command structures, enabled by communication developments, could provide the agility required. Fundamental exchanges could take place in space, denying access – with potentially catastrophic impacts on communications and navigation. This is yet another environment the operational commander will need to be increasingly cognisant of, particularly if operating systems become over reliant on space-based technologies and therefore vulnerable to attack.

There are exciting prospects ahead for operational commanders who relish such challenges. While these may appear daunting, other developments may ease the task in hand. Computer processing power has already been mentioned. The commander may also be able to exploit lighter logistic chains, courtesy of additive printing, or perhaps even hypersonic strategic air-lift. They may also make use

of other technologies that perhaps contribute to lowering the thresholds for military engagement, such as automated weapon systems. It is increasingly likely that the commander may need to exploit certain technologies and capabilities to fight merely to gain access to the global commons for deployment, let alone employment, of force – as these are likely to be more highly contested by 2035.

So, for the operational commander, the future operating environment will be more complex and ambiguous, from physical to electronic to human aspects. The jointery of today will still be needed; but we will habitually be working in an even more combined, joint, inter-agency, intra-governmental and multinational context to contend with the challenges. Operations conducted thus far will look relatively simple compared to some of those required in the future operating environment of 2035.

The '5Cs'

The '5Cs' (**congested, cluttered, contested, connected** and **constrained**) were introduced in DCDC's 2010 *Future Character of Conflict* to define the characteristics of the joint battlespace in 2014. FOE 35, while recognising the utility of the '5Cs' in some circumstances, recommends caution in their use. We should not assume that the '5Cs' will always apply to every environment. For example, consider an urban operating environment that is **congested** (densely populated) but relatively **uncluttered** (planned and orderly), or a peri-urban slum that could be **uncongested** (low density) but highly **cluttered** (informal and disorderly). The most challenging urban environments are likely to be both congested and cluttered-densely populated, informal settlements.

Considering ways in which the future operating environment may – and may not – be characterised by the '5Cs' can provide useful insights.

Congested. All environments (land, sea, air and space, cyber and the electromagnetic) will be populated by civilian, commercial and military activity. Armed forces may seek to avoid a densely populated or congested operating environment as it limits their freedom of manoeuvre. Yet we will need to bring military effects to bear wherever they are needed – congested spaces are not always avoidable. By contrast, violent conflict and natural disasters may cause operating environments to rapidly **decongest**. Although as activity migrates away from such areas, congestion may occur elsewhere.

Cluttered. Clutter leads to an inability to easily distinguish individuals, items or events, particularly in congested environments. Clutter will challenge our precision and discrimination in applying military effects.

This may ultimately result in reducing our legitimacy if we are unable to avoid civilian casualties or other unintended consequences. However, new technologies may provide us with the opportunity to **de-clutter** the operating environment, perhaps by finding patterns in a mass of information. Also, our adversaries may seek refuge in **uncluttered** remote or harsh terrain, where they rely upon physical isolation for protection.

Contested. All environments are likely to be contested, to varying degrees, out to 2035. The challenge will be in understanding where these contests are merely a result of **competition**, or where they could lead to **confrontation** or **conflict**. Failing to recognise the difference could lead to miscalculation.

Connected. The trends of interconnectivity and globalisation have resulted in dramatic increases in connectivity – across all environments. This is especially evident across the global commons and in cyberspace. However, these trends are not universal and could be reversed. Therefore, the potential for operating environments to be deliberately **disconnected** or simply **poorly connected** will remain, even out to 2035.

Constrained. Our legal and societal norms will continue to apply restraint to the conduct of military operations, particularly violent conflict, out to 2035. This will be particularly true where this applies to new technologies such as automated systems and novel weapons. Our potential adversaries may not be so constrained, and may operate **without restraint**.

Only by considering the numerous ways in which these characteristics interplay and overlap, if at all, can we still apply them to the future operating environment.

Acknowledgements

Wide external consultation and review has been conducted to ensure *Future Operating Environment 2035* is both comprehensive and independent in its view of the future. We have benefited enormously from the time and effort given generously by the individuals, organisations and institutions listed below. To all of those who contributed directly their valuable knowledge and expertise – we are extremely grateful for your participation and regret that space does not permit us to thank you all by name. We look forward to working with you again in the future.

UK Government departments

Cabinet Office:

National Security Secretariat.

Foreign and Commonwealth Office:

Conflict Department.

Defence and International Security Directorate.

Security Policy Department.

Home Office:

Office for Security and Counter-Terrorism.

Science, Engineering and Technology.

Department for International Development:

Conflict, Humanitarian and Security Department.
Stabilisation Unit.

Policy and Global Programmes.

Academe

Dr Tarak Barkawi, London School of Economics.

Dr Huw Bennett, University of Aberystwyth.

Dr Phil Clark, School of Oriental and African Studies, University of London.

Professor Paul Cornish, University of Exeter.

Professor Robert Cryer, University of Birmingham.

Dr Chris Donnelly (*independent*).

Dr Antulio Echeverria, Strategic Studies Institute, Army War College.

Dr Rob Johnson, Changing Character of Warfare, Oxford University.

Professor Mary Kaldor, London School of Economics.

Dr David Kilcullen (*independent*).

Professor Anthony King, University of Exeter.

William Owen (*independent*).

Dr Patrick Porter, University of Reading.

Dr Hugo Slim, University of Oxford.

Dr David Sloggett (*independent*).

Research and international organisations

Brookings Institution.

Rand Europe.

Royal Institute of International Affairs (Chatham House).

Royal United Services Institution.

International Institute of Strategic Studies.

International Committee of the Red Cross.

Industry

BAE Systems.

Boeing Defence UK.

Defence Growth Partnership.

KBR.

MBDA UK.

McKinsey & Company.

Selex/Finmeccanica UK.

Serco.

Shell.

International defence organisations

Department of Defence, Australia.

Capability Development Group.

Joint Concepts, Defence Preparedness Branch.

Defence Force Headquarters, New Zealand.

Future Force Development, Capability Branch.

North Atlantic Treaty Organisation.

Allied Command Transformation.

Department of Defence, Sweden.

Swedish Armed Forces Headquarters.

Forsvarets Forsknings Institut (FOI).

Swedish National Defence College, Department of Education, Sweden.

Department of Defense, United States of America.

Joint Staff J7.

National Intelligence Committee.

Naval Post Graduate School.

Army War College.

Air War College, Air University.

National Defense University.

Research, Development and Engineering Center, US Army.

Contact details

Strategic Trends Programme
Development, Concepts and Doctrine Centre
Shrivenham
Swindon
SN6 8RF

Email: dcdc-strategictrends@mod.uk

WITHDRAWN

Notes

WITHDRAWN

Notes

WITHDRAWN

WITHDRAWN

WITHDRAWN

