Chief of the Defence Staff, General Sir Nick Carter launches the Integrated Operating Concept

The Prime Minister I think has set a clear vision for the future of Global Britain. One where the UK is considered an outwardly looking, internationalist country, that acts as a burden-sharing and problem-solving nation, making a tangible contribution to tackling diplomatic and security challenges in our neighbourhood and beyond.

To do this though and particularly from our perspective in Defence, we must first understand that the threats to our national security, our values and our prosperity have evolved and diversified markedly. Our authoritarian rivals see the strategic context as a continuous struggle in which non-military and military instruments are used unconstrained by any distinction between peace and war. These regimes believe that they are already engaged in an intense form of conflict that is predominantly political rather than kinetic. Their strategy of 'political warfare' is designed to undermine cohesion, to erode economic, political and social resilience, and to compete for strategic advantage in key regions of the world.

Their goal is to win without going to war: to achieve their objectives by breaking our willpower, using attacks below the threshold that would prompt a war-fighting response. These attacks on our way of life from authoritarian rivals and extremist ideologies are remarkably difficult to defeat without undermining the very freedoms we want to protect. We are exposed through our openness.

The pervasiveness of information and rapid technological development have changed the character of warfare and of politics. We now have new tools, techniques and tactics that can be used to undermine political and social cohesion, and the means to make the connection to an audience ever more rapidly. Information is now democratised. It's available for everyone.

Our adversaries have studied our 'Western way of war', identified our vulnerabilities and modernised their own capabilities to target them. The campaigns of the last 30 years have been played out over global media networks. From the first Gulf War in the early 1990s to the air strikes in Bosnia and Kosovo, the response to the terrorist attacks on embassies in Kenya and Tanzania, and of course the campaigns in Iraq, Afghanistan and Libya – all have been watched closely by our rivals.

They saw that air power could penetrate deep into hostile territory and learned that we preferred to fight and strike targets from afar. They saw that this enhanced our natural aversion to putting people in harm's way. They watched how casualties, financial cost and length of time swayed domestic and public opinion and the effect that had on the legitimacy assuring the use of armed force.

So they learned how to improve their own resilience to absorb strikes; they developed anti access denial systems; they improved their maritime undersea capabilities; they developed long range missile systems; they integrated Electronic Warfare, swarms of drones with multiple fires and used these to defeat armour; they invested in space and cyber, recognising the importance we attach to global positioning and digitisation. And in Ukraine and Syria Russia has created battle laboratories from real life events to develop their tactics and battle harden a new generation of soldiers.

The US Department of Defence's latest annual report to Congress on military and security developments involving the People's Republic of China highlights that the PRC has marshalled the resources, technology, and political will over the past two decades to strengthen and modernize the People's Liberation Army. Including growing the largest maritime surface and sub-surface battle force in the world; an armoury of ground launched cruise and ballistic missiles – some of which have ten times the range of conventional ballistic missiles; one of the world's largest forces of advanced long range surface-to-air systems; and of course expanding the PRC's overseas military footprint.

They have also harnessed technologies and tactics that have outpaced the evolution of international law to avoid their actions being classified as conflict under the current definitions of international law. Authoritative PLA texts have argued that the ambiguous boundary between peace and war opens up opportunities for the military to achieve its ends, disguising its activities as civilian, and therefore peaceful.

China's new Strategic Support Force is designed to achieve dominance in the space and cyber domains. It commands satellite information attack and defence forces; electronic assault forces and Internet assault forces; campaign information operations forces, which include conventional electronic warfare forces, anti-radiation assault forces, and battlefield cyber warfare forces. All of this is available in the open domain.

Now, Western states draw legitimacy from respect for the rules, conventions and protocols of war. Where we see morals, ethics and values as a centre of gravity, authoritarian rivals see them as an attractive target. And all of a sudden the idea of 'lawfare' becomes a helpful tool in their inventory. The term 'lawfare' covers different meanings. In this context though, it entered national security parlance when it appeared in 'Unrestricted Warfare' – written on military strategy in the late 1990s by two PLA officers who used the term to refer to a nation's use of legalized international institutions to achieve strategic ends.

But 'lawfare' also applies to the challenge we have encountered in recent campaigns where we need to update our legal, ethical and moral framework to properly hold our forces to account if they break the law, while ensuring they have appropriate freedom of action to seize fleeting opportunities on the battlefield.

The COVID crisis has highlighted how the use of propaganda, data misuse, disinformation, and strategic influence is presenting complex and rapidly

evolving challenges for researchers, civil society, and of course for policymakers. And our autocratic rivals have utilised these techniques most effectively. The Australian Strategic Policy Institute is tracking how a range of actors are manipulating the information environment to exploit the COVID-19 crisis for strategic gain – including pro-Russian vaccine politics whose disinformation narratives are designed to permeate anti-vaccination social media groups.

Russia has used cyber and information attacks against its opponents regularly in the last few years. Notable examples included Ukraine's financial and energy sectors in 2017 and the Organisation for the Prohibition of Chemical Weapons in 2018. Iran and North Korea are following suit. And the online national security forum 'War on the Rocks' in their 'Digital Authoritarianism' series highlight Russia's hack-and-leak, 'kompromat' operations and the St. Petersburg-based Internet Research Agency troll farm which engages in sowing division abroad.

The WannaCry ransomware attack in May 2017 demonstrated how an attacker could rapidly achieve a global effect by spreading a virus through computers operating Microsoft Windows, holding user's files hostage, and demanding a Bitcoin ransom in return.

This idea of 'Digital Authoritarianism' also explores how the Chinese Communist Party is forging a future of mass surveillance and 'social credit scores' and is rapidly exporting these tools to other parts of the world. The recent Netflix documentary – A Social Dilemma – describes the way in which online interaction is subliminally influenced leading to the audience becoming unwittingly controlled.

Proxies, private military and security companies (PMCs) and militias are back in fashion as well. The recent report by the US Center for Strategic and International Studies on the expansion of Russian PMCs into security vacuums in parts of Africa, the Middle East, and South Asia is worth reflecting on.

Using companies, like the Wagner Group, Moscow can support state and non-state partners, extract resources, influence foreign leaders, and do so with plausible denial. Their military skills and capabilities lend a form of limited power projection, strengthening partners, establishing new military footholds, and altering regional balances to achieve strategic advantage. CSIS estimates that operations like these are underway in 30 countries across some four continents.

Our rivals typically tailor their activities to remain below obvious detection and response thresholds, and they often rely on the speed, volume and ubiquity of digital technology that characterizes the present age. And with an increased emphasis on creativity, ambiguity, and amplifying the cognitive elements of war, while dialling down the physical elements. Their way of warfare is strategic, it is synchronized and systematic – and our response must be too.

None of our rivals can afford to go to war as we define it. They want to win below that threshold. However, the stakes are high, the traditional

diplomatic instruments that have provided some measure of arms control and counter-proliferation have all but disappeared, with the last arms control treaty, New START potentially ending next February.

The upshot is that the threat of unwarranted escalation and therefore miscalculation between military protagonists is now clear and present. And as the competition for resources, bases and partners intensifies so the risks increase.

The Horn of Africa is a case in point. The Stockholm International Peace Research Institute sets out the growth of foreign military bases and a build-up of naval forces in the region since 2001 when the focus was on counterterrorism, counter piracy and of course peace support operations in the wake of 9/11. Currently a wide variety of international security actors operate there – from Europe, the United States, the Middle East, the Gulf, and Asia and international networks of military facilities and naval deployments together link the Horn to security developments in the Middle East and the Gulf, the Indian Ocean and Asia Pacific, as well as in other parts of Africa. The level of military engagement is matched in the Eastern Mediterranean where the potential for misunderstanding is significant.

And, as we look down the barrel of a global recession it's worth reflecting on how often financial crises lead to security crises.

So, what should be our response to this ever more complex and dynamic strategic context? My view is that more of the same will not be enough. We must fundamentally change our thinking if we are not to be overwhelmed.

Hence we are launching this Integrated Operating Concept. It has several big ideas:

First of all, it makes a distinction between 'operating' and 'war-fighting'. In an era of persistent competition our deterrent posture needs to be more dynamically managed and modulated. This concept therefore introduces a fifth 'c' – that of competition – to the traditional deterrence model of comprehension, credibility, capability and communication. This recognises the need to compete below the threshold of war in order to deter war, and to prevent one's adversaries from achieving their objectives in fait accompli strategies. As we have seen in the Crimea, Ukraine, Libya and further afield.

Competing involves a campaign posture that includes continuous operating on our terms and in places of our choosing. This requires a mindset that thinks in several dimensions to escalate and deescalate up and down multiple ladders – as if it were a spider's web. One might actively constrain in the cyber domain to protect critical national infrastructure in the maritime Domain.

This campaign posture must be dynamically managed and there must be a preparedness to allocate consistent means over longer term horizons, while adjusting the ways to anticipate a rival's response. The ways will include actions being communicated in a manner that may well test the traditional limits of statecraft.

This posture will be engaged and forward deployed – armed forces much more in use rather than dedicated solely for contingency – with training and exercising being delivered as operations. It will involve capacity building and engagement in support of countries that need our support. This could include partnered operations against common threats – particularly violent extremism. And this may involve combat operations.

It will also place a premium on building alliances and improving interoperability to make us more 'allied by design' and thus able to burden share more productively.

It is important to emphasise that the willingness to commit decisively hard capability with the credibility to war fight is an essential part of the ability to operate and therefore of deterrence.

The second important idea is that we cannot afford any longer to operate in silos – we have to be integrated: with allies as I have described, across Government, as a national enterprise, but particularly across the military instrument. Effective integration of maritime, land, air, space and cyber achieves a multi-Domain effect that adds up to far more than simply the sum of the parts – recognising – to paraphrase Omar Bradley – that the overall effect is only as powerful as the strength of the weakest Domain.

And third we have to modernise. We must chart a direction of travel from an industrial age of platforms to an information age of systems.

Warfare is increasingly about a competition between hiding and finding. It will be enabled at every level by a digital backbone into which all sensors, effectors and deciders will be plugged. This means that some industrial age capabilities will increasingly have to meet their sunset to create the space for capabilities needed for sunrise. The trick is how you find a path through the night. We know this will require us to embrace combinations of information-centric technologies. But predicting these combinations will be challenging.

We will have to take risk, accept some failure and place emphasis on experimentation by allocating resources, force structure, training and exercise activity to stimulate innovation in all lines of development, with a responsive commercial function at the leading edge. This will enable adaptive exploitation as opportunities become clear and allow better financial control.

Throughout we must recognise that the nature of war doesn't change – it is always visceral, it is always violent, and it always involves interaction between people, in the final analysis one has to go close and personal with one's enemy. So, while this Integrated Operating Concept places a premium on operating, it also places a premium on adaptability – the ability to adapt to war fight. And this in turn emphasises the importance of our people – who have always been, and always will be, our adaptive edge.