Chief of Defence Staff at RUSI Annual lecture

It's a great pleasure once again to be giving the annual CDS Christmas Lecture at RUSI, even if this year it feels somewhat weird doing so in an empty room and in a temporary building.

But, it has been quite a year – particularly with the announcement last month by the Prime Minister of a £24.1-billion uplift in defence spending. This is the most significant increase since the end of the Cold War, and it reverses, I think, a long period of decline. The rationale for it has been firmly established in the development of the Government's Integrated Review of Foreign, Defence, Security and International Development Policy which will be published early next year, and we have already seen a new foreign policy posture emerging that indicates the direction of travel, Magnitsky and Hong Kong being obvious examples.

When I spoke last year not many of us would have predicted the COVID-19 pandemic. But even before we were hit by it, I would have described the strategic context as uncertain, complex and dynamic; with the defining condition being one of chronic instability.

COVID-19 has brought all this more sharply into focus. It has exposed some stark choices as historian Yuval Noah Harari (the author of the bestselling book Sapiens) presciently observed at the beginning of the crisis: "we face two particularly important choices. The first is between totalitarian surveillance and citizen empowerment. The second is between nationalist isolation and global solidarity."

The absence of global solidarity and shared responsibility has been particularly striking. Countries have turned in on themselves as have many alliances. IISS noted recently that the pandemic had accelerated the atomisation of international society. There have been some examples of global cooperation – notably the Gavi Vaccine Alliance – but in general the multi-lateral global system has not unified nations as positively as it once did. Indeed, in some institutions – the World Health Organisation for example – it has been actively undermined.

The Coronavirus has revealed the nature of global competition and conflict very starkly. We saw some extraordinary international behaviour in the race for PPE and ventilators in the early stages of the crisis. We have seen misinformation which confuses and undermines trust and disinformation which deliberately polarizes public debate on topics related to COVID-19. Russian efforts to undermine the Oxford AstraZenica vaccine as a 'monkey vaccine' for economic and reputational purposes. Which of course reveals the importance attached to the moral authority that can be wielded through science to persuade others to gravitate to your ideological sphere of influence.

What we have also seen more clearly is the evolving Digital Great Game that

is playing out. China's Digital Silk Road will probably be the most influential element of the Belt and Road Initiative. The online financial newspaper Nikkei Asia observed that BeiDou (that stands for Big Dipper as it translates), China's recently launched alternative to GPS, provides more accurate coverage than the American version in 165 of 195 capital cities around the world. Given that much of the smartphone economy is built to be compatible with a specific location service, there is an obvious connection with all the other services needed within smart cities, and, as Y Yuval Noah Harari implies, the potential for totalitarian surveillance.

As the internet risks fragmenting, China is trying to draw much of the non-rich world into its sphere of influence by providing the digital infrastructure that companies and services are built on. Location services are but only one aspect. Huawei is being shut out of 5G only in the rich world. Nikkei Asia also says that China has overtaken the US to become the country with the most data crossing its borders. And the Financial Times recently reported that China has used its growing influence at the UN to shape technical standards for facial recognition and surveillance tech through the International Telecommunication Union, a UN body. A sign perhaps of what is to come in the China Standards 2035 plan when it is released.

And to Yuval Harari's point about citizen empowerment, it has been striking how many so-called democracies have used the pandemic as an opportunity to enhance their power in authoritarian ways. This trend was evident even before the virus hit. According to Freedom House the democratic downturn was particularly steep in the last five years which was the first 5 year period since 1975 in which more countries transitioned to autocracy than to democracy.

Now, I'm sure we will deduce a number of other lessons from this crisis. There will be lessons for all in how risk registers are treated, in how health care is delivered; I suspect stockpiles will no longer be a dirty word and supply chain resilience will be something to be proud of. And we should expect greater emphasis on climate, the environment, net zero and green renewal in defence as well I would suggest.

Now, I've been very proud of how the armed forces have contributed to the crisis, delivering innovative solutions to complex problems, supporting those on the front line, and providing a sense of reassurance at key moments – and all of it done with impressive humility and positive energy. As well as delivering a high intensity of operational activity without a break in step.

What we have seen this year with COVID-19 is a reminder that the threats to our national security, our values and our prosperity have evolved and diversified markedly. Our authoritarian rivals (I use this term to make the point that this is not necessarily about 'enemies') they 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 military. 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 very 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.

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 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 they learned that we preferred to find 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 air defence systems that deny our freedom of action; they improved their maritime undersea capabilities; they developed long range missile systems; they integrated Electronic Warfare, swarms of drones connected digitally to missile systems and used these to defeat tanks; 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 situations to develop tactics and battle harden a new generation of soldiers. And they proliferated many of these new systems to their proxies.

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 they have grown the largest maritime surface and underwater fleet in the world; they deployed ground launched cruise and ballistic missiles, with markedly longer ranges and lethality; they developed one of the world's largest forces of advanced long range surface-to-air systems; and expanded 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 definitions of international law. 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; and even cyber warfare forces.

Western states draw legitimacy from their 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. The idea of 'lawfare' becomes a helpful tool in their inventory. Now, the term 'lawfare' covers different meanings. In this context it entered national security parlance when it appeared in 'Unrestricted Warfare' – a book written on military strategy in 1999 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' from our perspective 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. We also need to win the competition with authoritarian rivals to define the right legal and ethical framework for emerging and disruptive technology, not least autonomous weapons and cyber. But, also the threat, which I will come back to from Digital authoritarianism and totalitarian surveillance.

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. And more recently, the planned cyber-attack on the Tokyo Olympics as called out by our own National Cyber Security Centre, as well as the recent attack against US government systems. 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.

'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, mercenaries and militias are back in fashion as well. The recent report by the US Center for Strategic and International Studies (CSIS) on the expansion of Russian mercenaries into security vacuums in parts of Africa, the Middle East, and South Asia is worth a read. It reveals how mercenaries, like Moscow's Wagner Group, can be used to support state and non-state partners, extract resources, influence foreign leaders, and do so with plausible denial. CSIS estimates that operations like these are underway in 30 countries across 4 continents.

There is, I would suggest, a clear trend towards toward military action that uses the cognitive elements of war with arms-length instruments like drones and mercenaries to provide a plausible degree of deniability and strategic ambiguity – thus enabling intervention without the risk of entanglement. Their way of warfare is strategic, it is synchronized, and it is systematic.

But 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 and counter proliferation treaty, New START potentially ending next February. The upshot is that the threat of unwarranted escalation and therefore miscalculation is clear and present.

Our response must be strategic, it must integrate all of the instruments of statecraft – ideology, reputation, diplomacy, finance, trade policy and military power – if it is to be effective. Hence the importance of the cross-cutting nature of the Government's Integrated Review. It is also encouraging to see that the recently published NATO Independent Reflections Group recommends expanding NATO engagement to include Ministers of Finance, Interior, Infrastructure and Research.

Next I would say as a military officer that alongside Sun Tzu's observation that "the supreme art of war is to subdue the enemy without fighting" we should remember our Clausewitz. "The first, the supreme, the most far-reaching act of judgement", he wrote, "that the statesman and commander have to make is to establish by that test the kind of war on which they are embarking; neither mistaking it for, nor trying to turn it into, something that is alien to its nature."

Now, I'm not suggesting we are about to go to 'war' however we need to define the nature of this contest, what victory looks like, and then match the ways and means to achieve the ends. And I suggest that – the means to control others – principally through the application of technology – is the crux of the matter. Because control of digital technology allows our rivals to take over our way of life. Defending it will likely require the creation of an alternative digital sphere of influence, alongside the terrestrial one.

What's needed is a catalyst somewhat like George Kennan's 'long telegram' in which he observed that peaceful coexistence with the Soviet Union in 1946 was unlikely to work. This led to the Truman Doctrine of containment and which provided the basis of US and Western strategy throughout the Cold War.

Maybe what last month's important NATO Reflections Group's report had to say about China could stimulate our thinking:

"NATO must devote much more time, political resources, and action to the security challenges posed by China – based on an assessment of its national capabilities, economic heft, and the stated ideological goals of its leaders. It needs to develop a political strategy for approaching a world in which China will be of growing importance through to 2030. The Alliance should infuse the China challenge throughout existing structures and consider establishing a consultative body to discuss all aspects of Allies' security interests, vis-a-vis China. It must expand efforts to assess the implications

of China's technological development and monitor and defend against any Chinese activities that could impact collective defence, military readiness or resilience in the Supreme Allied Commander Europe's (SACEUR) Area of Responsibility."

Now, the complex geostrategic context I have described is why we have launched a new Integrated Operating Concept in late September. It is defence's input to the Integrated Review. It has several big ideas pertaining to the role of the military instrument. It is arguably the most significant change in British military thought in generations. In the past we would have structured and organised our armed forces to war fight and adapted to do everything else. What this Concept does is to recognise that our rivals seek to win without resorting to war – so we need to be structured to outmatch them – while being able to adapt to war fight if necessary.

So, first and foremost the Concept updates our thinking about deterrence. Developing the point about our opponents seeking to win without embarking on a 'hot' war, it makes a distinction between 'war-fighting' and 'operating'. You cannot afford to be passive in an era of persistent competition. Our deterrent posture needs to be more imaginative and dynamically managed. It therefore introduces a fifth 'c' – that of competition – to the traditional deterrence model of comprehension, capability, credibility and communication.

This recognises that competition below the threshold of war is not only necessary to deter war, it is also necessary to prevent one's adversaries from achieving their objectives in fait accompli strategies as we have seen in the Crimea, Ukraine, Libya and the South China Sea for example. It is also important to emphasise that the willingness to commit decisively, hard capability with the credibility to war fight with a conviction that shows we mean business is an essential part of the ability to operate and therefore of deterrence.

Competing involves a posture of dynamic campaigning. This requires us to think for the long term about where and how we apply the ways and means we need – like our authoritarian rivals do, and can do, given the persistence of their leadership. It also requires us to think in several dimensions, perhaps escalating in the cyber dimension while toning down our posture in the air or maritime dimension, while messaging a tone of reduced aggression in the information dimension. Nowadays it's not so much a ladder, but a spider's web of multiple ladders, because escalation dominance is now much harder to manage given the complexity of weaponry – long range conventional missiles, space and cyber for example. To bring this to life we will run a number of exercises next year to test our resilience and our ability to navigate crisis.

We must expect our rivals continuously to refine and improve their methods for promoting mischief and political disarray in our societies, while seeking to lure our traditional partners into their sphere of influence. We need to invest more in our network of Defence Attaches, embedded alongside our FCDO missions abroad to provide us with the insight and understanding, and intelligence and warning we need to adjust our posture and out manoeuvre our rivals.

This posture will be engaged and forward deployed – to defend ourselves and our allies, our armed forces much expect to spend far more time deployed and based abroad training and exercising in the regions most exposed to the threat. We will think of this activity as being operational. It will involve capacity building of all kinds – civil and military – building close relationships with nations that seek our support. Much of it will be about our soft power – training, education, doctrine and accreditation – underscored by our military credibility and expertise.

This could include partnered operations against common threats – particularly violent extremism – and this may involve combat operations. And it will form an element of the Government's broader regional strategies. For example, the current deployment of a battle group to Mali as part of the MINUSMA mission is but part of a broader West Africa strategy as well as a UK desire to help reinforce UN peacekeeping.

We field and manage requests from other countries for this sort of activity through our network of attaches and – in the Caribbean and the Gulf – through annual meetings with my opposite numbers to ensure we are meeting the local requirement. Using the Gulf to illustrate this posture, we have the Royal Navy's HMS MONTROSE forward deployed alongside Mine Counter Measures Force. We operate in partnership with the Gulf countries as part of the Combined Maritime Force and the International Maritime Security Construct (IMSC) that maintains freedom of navigation for commercial ships throughout the region.

In the Air we are contributing to the air defence of Saudi Arabia and we are currently exercising Typhoons with the Qatari Air Force, which has pilots embedded in the RAF's 12 Squadron. We have a Joint Defence Agreement with Oman where Army battle groups will train alongside the Omanis at a new Joint Training facility on the coast at Ras Madrakah. The neighbouring Duqm port has become an invaluable logistics base that will facilitate Royal Navy deployments in the Indian Ocean and its dry dock facility is capable of supporting our two new aircraft carriers.

This campaigning posture for our armed forces also addresses state threats. The most serious of these in the Euro Atlantic area is of course Russia and we have seen recently that Moscow is determined to test Britain and our NATO allies. The Russian regime's increasingly assertive activity is almost certainly influenced by problems at home. They are wrestling with their own sense of 'imperial overstretch' as their near abroad becomes increasingly restive.

The week before last Russia assembled ten or so warships and combat aircraft from the Northern, Baltic and Black Sea fleets in a show of force in the waters off the British and Irish coasts. They are flexing their muscles in our own back yard within an ostentation they have not displayed since the Cold War. Deterring these threats, signalling to the Russian regime that we shall not tamely acquiesce should they escalate requires conventional hard power – warships and aircraft – as well as less conventional capabilities like cyber. And it requires us to hold their backyard at risk whether that's in the Barents Sea, the High North, the Baltic or the Black Sea.

Hence our campaign posture emphasises strengthening relations with our friends, constantly improving the readiness of our armed forces to operate alongside allies, with compatible weapons, communications systems and procedures – a key advantage we have over our rivals – to make us more 'allied by design' and thus able to burden share more constructively. NATO is at the heart of this. I referred earlier to the NATO Reflections Process. Along with taking a broader view on the utility of other levers of statecraft, it recommends strengthening partnerships, an increasing focus on hybrid threats, investing to maintain the technological edge, stronger strategic communications and an update to NATO's 2010 Strategic Concept.

Our Integrated Operating Concept has influenced NATO's new concept for Deterrence and Defence of the Euro Atlantic region which seeks to bring policy and military strategy closer together for an era of sharper political competition. Alongside this our Integrated Operating Concept is also influencing the new NATO Warfighting Capstone Concept that provides a north star for force and capability development. It recognises the very dynamic nature of the operating environment – and it seeks to create the conditions for the Alliance to 'out-think, out-excel, out-fight – and particularly 'out-pace' our adversaries. It needs to lead to a more dynamic NATO force planning process that incentivises allies to modernise. We will continue to be one of only a small number of NATO allies who bring to bear nuclear, cyber, precision strike weapons, 5th generation aircraft, surface and underwater capability, a Corps HQ, an agile manoeuvre division all enabled by information warfare.

Now, the second important idea in the Integrated Operating Concept is that word 'integration'. We cannot afford 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. This is about effective integration of the capabilities of the Navy, the Army, the Air Force and through Strategic Command, and our cyber and intelligence organisations (or for defence aficionados listening to this lecture – the maritime, land, air, space and cyber domains).

The National Cyber Force is a prominent example of how defence is working in partnership with GCHQ to deliver cutting edge capability. This integration achieves a multi-Domain effect that amounts to far more than simply the sum of the parts – recognising – to paraphrase General Omar Bradley the first US Chairman of the Joint Chiefs of Staff – that the national fighting machine is only as powerful as its weakest element (or Domain).

And the third idea in the concept is how we'll modernise, and this is where the Prime Minister's announcement is particularly helpful, because for the first time that I can remember, we now have planning certainty for the next 10 years. This will allow us to 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 backbone will enable all of the five operational domains to be linked together and integrated with each other

from the strategic level down to the ship's captain or platoon commander. It will deliver a secure cloud of accessible data (think smart phone) this will enable artificial intelligence, robotics and synthetics – with decision making at the speed of relevance.

Software will be as important as hardware in determining what our armed forces will be capable of in the future and the idea of a new digital foundry that the Prime Minister referred to will provide the technical know-how to allow rapid adaptation.

This direction of travel means that some industrial age capabilities will have to meet their 'sunset' to create the space for capabilities needed for 'sunrise'. This will be an incremental process, recognising that in the emerging operating environment some sunset capabilities will be useful in a mix of 'high-low' systems but will increasingly become vulnerable in a war fighting context.

The trick is how you find a path through the night as you develop capability from sunset to sunrise. We know this will require us to embrace combinations of information-centric technologies. But predicting the right mix will be tough. We shall have to take risks, seek a right sometimes to fail. We need to experiment by allocating resources, force structure, training and exercise activity to stimulate innovation. We need to work more imaginatively with commercial companies that make our systems and with centres of learning and industry at large, utilising the £1.5-billion of research and development money the Prime Minister announced. If we do this right we can perhaps avoid some of the expensive mistakes that have caused embarrassment for defence procurement in the past.

Each of the Services and Strategic Command, and therefore the operational domains are at a different stage of their development. The Navy's future is clearly charted through the national ship building strategy the Prime Minister announced and the steady drumbeat of submarine delivery, as well as its imaginative thinking around autonomy. The RAF has a route to the future with the Future Combat Air System or Tempest, which is an exciting technology programme that will take us to the next generation of combat air capability. And the Army will undergo its most comprehensive modernisation since the 1980s era of Air Land. It will become better able to fight at reach, with layered target acquisition and precision fires; its air defence capability will be markedly improved; it will experiment its way to robotic and autonomous capabilities; and it will transform its global network to see more soldiers involved in the persistent engagement I described earlier. The performance of all three Services will be enhanced by our investment through Strategic Command in space and cyber.

Throughout – we must recognise that the nature of war does not change – it is always about violence, guts, people. When you're up against a determined opponent on the battlefield you have to go close and personal with your enemy – I'm afraid it's too early to plot the demise of the tank … 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.

I have said it before – we are in a period of phenomenal change – more widespread, rapid and profound than humanity has experienced outside of world war. And it is more sustained than the two world wars of the last century combined – and the pace is forever quickening. Our fundamental and long held assumptions are being disrupted on a daily basis. Modernising will only get us so far – what is needed is a step-change in how we fight; in how we run the business; in how we develop our talent; in how we acquire our equipment; and in how we provide support – this requires a transformation.

This scale of change must be led from the top, but equally, change at this pace must also be delivered bottom-up, by the generation who have grown up with digital technology, and who are far more comfortable with the modern world than their leaders. We must empower our young sailors, soldiers, airmen and airwomen to unlock their potential. But we will not deliver change of this scale and breadth on our own – this must be a shared national enterprise, in which the British people understand us, empathise with us and support our purpose. We shall make our share of mistakes, because that is what human beings do, both in peace and war, but we'll learn from them. We shall surprise and perhaps dismay some people who expect us now, as sometimes in the past, to be preparing to fight the last war.

Our business is instead with the next one, and with arming, training and equipping ourselves to fight if we must, but if possible, to convince our prospective adversaries that the game would not be worth the candle.

Thank you.