The next war

The growing danger of great-power conflict

The Economist: January 25, 2018

How shifts in technology and geopolitics are renewing the threat

IN THE past 25 years war has claimed too many lives. Yet even as civil and religious strife have raged in Syria, central Africa, Afghanistan and Iraq, a devastating clash between the world's great powers has remained almost unimaginable.

No longer. Last week the Pentagon issued a new national defence strategy that put China and Russia above jihadism as the main threat to America. This week the chief of Britain's general staff warned of a Russian attack. Even now America and North Korea are perilously close to a conflict that risks dragging in China or escalating into nuclear catastrophe.

As our special report this week on the future of war argues, powerful, long-term shifts in geopolitics and the proliferation of new technologies are eroding the extraordinary military dominance that America and its allies have enjoyed. Conflict on a scale and intensity not seen since the second world war is once again plausible. The world is not prepared.

The pity of war

The pressing danger is of war on the Korean peninsula, perhaps this year. Donald Trump has vowed to prevent Kim Jong Un, North Korea's leader, from being able to strike America with nuclear-armed ballistic missiles, a capability that recent tests suggest he may have within months, if not already. Among many contingency plans, the Pentagon is considering a disabling pre-emptive strike against the North's nuclear sites. Despite low confidence in the success of such a strike, it must be prepared to carry out the president's order should he give it.

Even a limited attack could trigger all-out war. Analysts reckon that North Korean artillery can bombard Seoul, the South Korean capital, with 10,000 rounds a minute. Drones, midget submarines and tunnelling commandos could deploy biological, chemical and even nuclear weapons. Tens of thousands of people would perish; many more if nukes were used.

This newspaper has argued that the prospect of such horror means that, if diplomacy fails, North Korea should be contained and deterred instead. Although we stand by our argument, war is a real possibility. Mr Trump and his advisers may conclude that a nuclear North would be so reckless, and so likely to cause nuclear proliferation, that it is better to risk war on the Korean peninsula today than a nuclear strike on an American city tomorrow.

Even if China stays out of a second Korean war, both it and Russia are entering into a renewal of great-power competition with the West. Their ambitions will be even harder to deal with than North Korea's. Three decades of unprecedented economic growth have provided China with the wealth to transform its armed forces, and given its leaders the sense that their moment has come. Russia, paradoxically, needs to assert itself now because it is in long-term decline. Its leaders have spent heavily to restore Russia's hard power, and they are willing to take risks to prove they deserve respect and a seat at the table.

Both countries have benefited from the international order that America did most to establish and guarantee. But they see its pillars—universal human rights, democracy and the rule of law—as an imposition that excuses foreign meddling and undermines their own legitimacy. They are now revisionist states that want to challenge the status quo and look at their regions as spheres of influence to be dominated. For China, that means East Asia; for Russia, eastern Europe and Central Asia.

Neither China nor Russia wants a direct military confrontation with America that they would surely lose. But they are using their growing hard power in other ways, in particular by exploiting a "grey zone" where aggression and coercion work just below the level that would risk military confrontation with the West. In Ukraine Russia has blended force, misinformation, infiltration, cyberwar and economic blackmail in ways that democratic societies cannot copy and find hard to rebuff. China is more cautious, but it has claimed, occupied and garrisoned reefs and shoals in disputed waters.

China and Russia have harnessed military technologies invented by America, such as long-range precision-strike and electromagnetic-spectrum warfare, to raise the cost of intervention against them dramatically. Both have used asymmetric-warfare strategies to create "anti-access/area

denial" networks. China aims to push American naval forces far out into the Pacific where they can no longer safely project power into the East and South China Seas. Russia wants the world to know that, from the Arctic to the Black Sea, it can call on greater firepower than its foes—and that it will not hesitate to do so.

If America allows China and Russia to establish regional hegemonies, either consciously or because its politics are too dysfunctional to muster a response, it will have given them a green light to pursue their interests by brute force. When that was last tried, the result was the first world war.

Nuclear weapons, largely a source of stability since 1945, may add to the danger. Their command-and-control systems are becoming vulnerable to hacking by new cyber-weapons or "blinding" of the satellites they depend on. A country under such an attack could find itself under pressure to choose between losing control of its nuclear weapons or using them.

Vain citadels

What should America do? Almost 20 years of strategic drift has played into the hands of Russia and China. George W. Bush's unsuccessful wars were a distraction and sapped support at home for America's global role. Barack Obama pursued a foreign policy of retrenchment, and was openly sceptical about the value of hard power. Today, Mr Trump says he wants to make America great again, but is going about it in exactly the wrong way. He shuns multilateral organisations, treats alliances as unwanted baggage and openly admires the authoritarian leaders of America's adversaries. It is as if Mr Trump wants America to give up defending the system it created and to join Russia and China as just another truculent revisionist power instead.

America needs to accept that it is a prime beneficiary of the international system and that it is the only power with the ability and the resources to protect it from sustained attack. The soft power of patient and consistent diplomacy is vital, but must be backed by the hard power that China and Russia respect. America retains plenty of that hard power, but it is fast losing the edge in military technology that inspired confidence in its allies and fear in its foes.

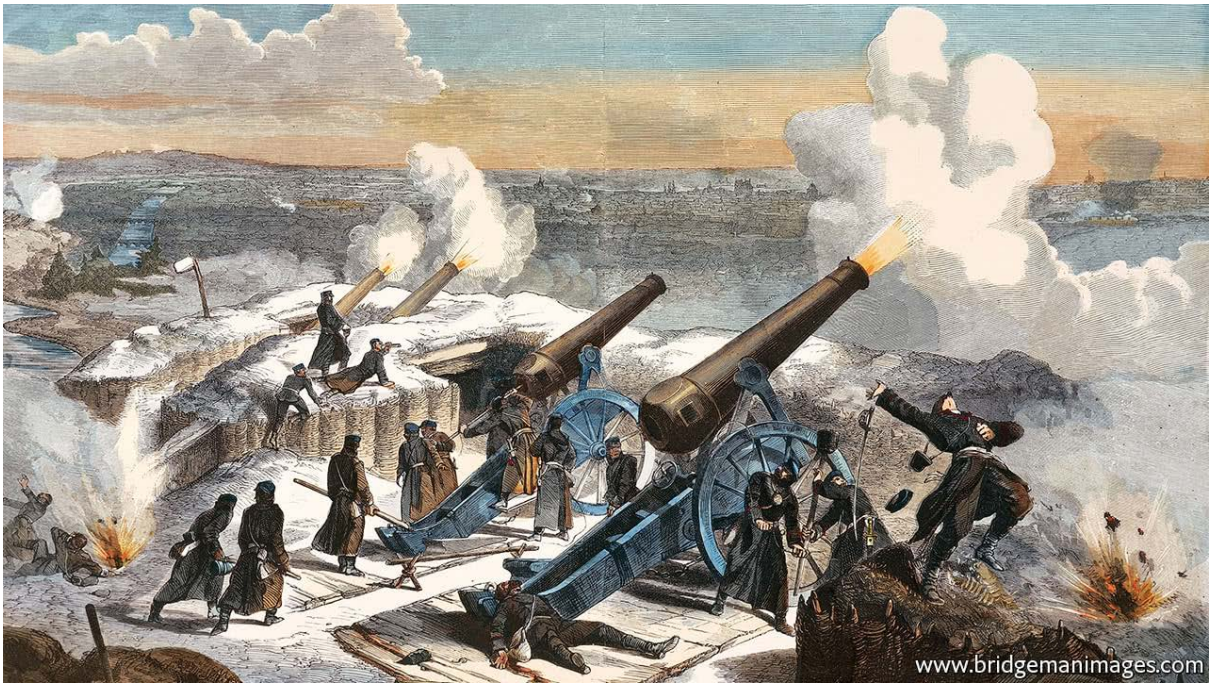
To match its diplomacy, America needs to invest in new systems based on robotics, artificial intelligence, big data and directed-energy weapons. Belatedly, Mr Obama realised that America required a concerted effort to regain its technological lead, yet there is no guarantee that it will be the first to innovate. Mr Trump and his successors need to redouble the effort.

The best guarantor of world peace is a strong America. Fortunately, it still enjoys advantages. It has rich and capable allies, still by far the world's most powerful armed forces, unrivalled war-fighting experience, the best systems engineers and the world's leading tech firms. Yet those advantages could all too easily be squandered. Without America's commitment to the international order and the hard power to defend it against determined and able challengers, the dangers will grow. If they do, the future of war could be closer than you think.

The new battlegrounds

The future of war

War is still a contest of wills, but technology and geopolitical competition are changing its character, argues Matthew Symonds



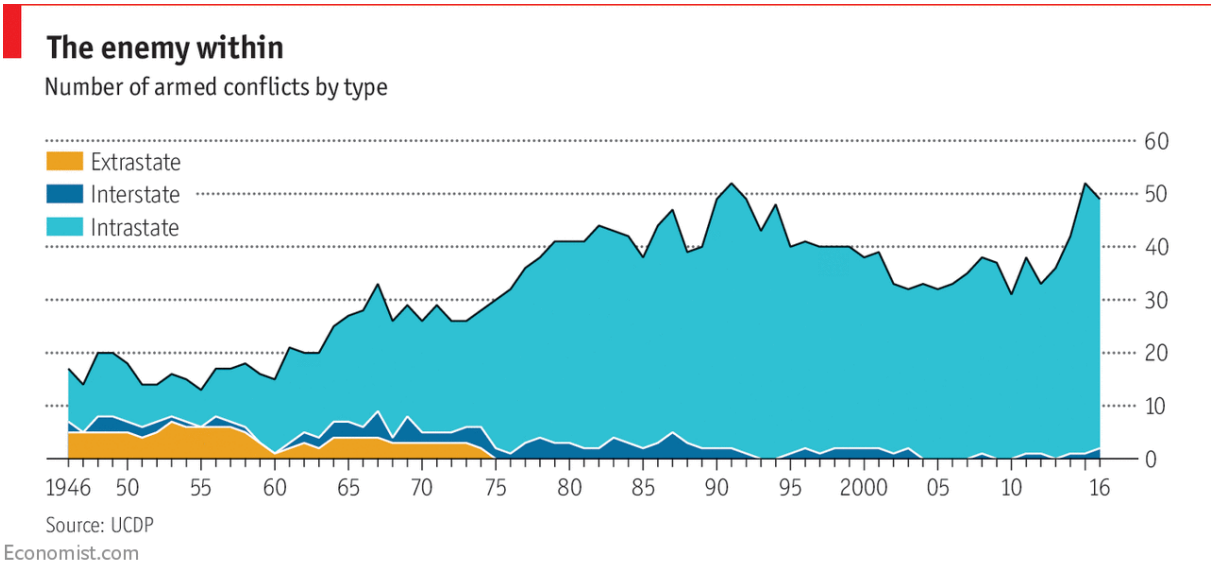
IN THE PAST, predictions about future warfare have often put too much emphasis on new technologies and doctrines. In the 19th century the speedy victory of the Prussian army over France in 1870 convinced European general staffs that rapid mobilisation by rail, quick-firing artillery and a focus on attack would make wars short and decisive. Those ideas were put to the test at the beginning of the first world war. The four years of trench warfare on the western front proved them wrong.

In the 1930s it was widely believed that aerial bombardment of cities would prove devastating enough to prompt almost immediate capitulation. That forecast came true only with the invention of nuclear weapons a decade later. When America demonstrated in the first Gulf war in 1990-91 what a combination of its precision-guided munitions, new intelligence, surveillance and reconnaissance methods, space-based communications and stealth technology could achieve, many people assumed that in future the West would always be able to rely on swift, painless victories. But after the terrorist attacks on America on September 11th 2001, wars took a different course.

This special report will therefore offer its predictions with humility. It will also limit them to the next 20 years or so, because beyond that the uncertainties become overwhelming. And it will not speculate about the clear and present danger of war breaking out over North Korea’s nuclear

weapons, which with luck can be contained. Instead, it will outline the long-term trends in warfare that can be identified with some confidence.

In the past half-century wars between states have become exceedingly rare, and those between great powers and their allies almost non-existent, mainly because of the mutually destructive power of nuclear weapons, international legal constraints and the declining appetite for violence of relatively prosperous societies. On the other hand, intrastate or civil wars have been relatively numerous, especially in fragile or failing states, and have usually proved long-lasting. Climate change, population growth and sectarian or ethnic extremism are likely to ensure that such wars will continue.



Increasingly, they will be fought in urban environments, if only because by 2040 two-thirds of the world's population will be living in cities. The number of megacities with populations of more than 10m has doubled to 29 in the past 20 years, and each year nearly 80m people are moving from rural to urban areas. Intense urban warfare, as demonstrated by the recent battles for Aleppo and Mosul, remains grinding and indiscriminate, and will continue to present difficult problems for well-meaning Western intervention forces. Technology will change war in cities as much as other types of warfare, but it will still have to be fought at close quarters, block by block.

Even though full-scale interstate warfare between great powers remains improbable, there is still scope for less severe forms of military competition. In particular, both Russia and China now seem unwilling to accept the international dominance of America that has been a fact of life in the 20 years since the end of the cold war. Both have an interest in challenging the American-sponsored international order, and both have recently shown that they are prepared to apply military force to defend what they see as their legitimate interests: Russia by annexing Crimea and destabilising Ukraine, and China by building militarised artificial islands and exerting force in disputes with regional neighbours in the South and East China Seas.

In the past decade, both China and Russia have spent heavily on a wide range of military capabilities to counter America's capacity to project power on behalf of threatened or bullied allies. In military jargon, these capabilities are known as anti-access/area denial or A2/AD. Their aim is not to go to war with America but to make an American intervention more risky and more costly. That has increasingly enabled Russia and China to exploit a "grey zone" between war and peace. Grey-zone operations aim to reap either political or territorial gains normally associated with overt military aggression without tipping over the threshold into open warfare with a powerful adversary. They are all about calibration, leverage and ambiguity. The grey zone particularly lends itself to hybrid warfare, a term first coined about ten years ago. Definitions vary, but in essence it is a blurring of military, economic, diplomatic, intelligence and criminal means to achieve a political goal.

The main reason why big powers will try to achieve their political objectives short of outright war is still the nuclear threat, but it does not follow that the "balance of terror" which characterised the cold war will remain as stable as in the past. Russia and America are modernising their nuclear forces at huge expense and China is enlarging its nuclear arsenal, so nuclear weapons may be around until at least the end of the century. Both Vladimir Putin and Donald Trump, in their very different ways, enjoy a bit of nuclear sabre-rattling. Existing nuclear-arms-control agreements are fraying. The protocols and understandings that helped avert Armageddon during the cold war have not been renewed.

Russia and China now fear that technological advances could allow America to threaten their nuclear arsenals without resorting to a nuclear first strike. America has been working at a concept known as Conventional Prompt Global Strike (CPGS) for over a decade, though weapons have yet to be deployed. The idea is to deliver a conventional warhead with a very high degree of accuracy, at hypersonic speeds (at least five times faster than the speed of sound), through even the most densely defended air space. Possible missions include countering anti-satellite weapons; targeting the command-and-control nodes of enemy A2/AD networks; attacking the nuclear facilities of a rogue proliferator such as North Korea; and killing important terrorists. Russia and China claim that CPGS could be highly destabilising if used in conjunction with advanced missile defences. Meanwhile they are developing similar weapons of their own.

Other potential threats to nuclear stability are attacks on nuclear command-and-control systems with the cyber- and anti-satellite weapons that all sides are investing in, which could be used to disable nuclear forces temporarily. Crucially, the identity of the attacker may be ambiguous, leaving those under attack uncertain how to respond.

Rise of the killer robots

At least the world knows what it is like to live in the shadow of nuclear weapons. There are much bigger question-marks over how the rapid advances in artificial intelligence (AI) and deep learning will affect the way wars are fought, and perhaps even the way people think of war. The big concern is that these technologies may create autonomous weapons systems that can make choices about killing humans independently of those who created or deployed them. An international "Campaign to Stop Killer Robots" is seeking to ban lethal autonomous weapons before they even come into existence. A letter to that effect, warning against a coming arms race

in autonomous weapons, was signed in 2015 by over 1,000 AI experts including Stephen Hawking, Elon Musk and Demis Hassabis.

Such a ban seems unlikely to be introduced, but there is room for debate about how humans should interact with machines capable of varying degrees of autonomy, whether in the loop (with a human constantly monitoring the operation and remaining in charge of critical decisions), on the loop (with a human supervising machines that can intervene at any stage of the mission) or out of the loop (with the machine carrying out the mission without any human intervention once launched). Western military establishments insist that to comply with the laws of armed conflict, a human must always be at least on the loop. But some countries may not be so scrupulous if fully autonomous systems are seen to confer military advantages.

Such technologies are being developed around the globe, most of them in the civil sector, so they are bound to proliferate. In 2014 the Pentagon announced its "Third Offset Strategy" to regain its military edge by harnessing a range of technologies including robotics, autonomous systems and big data, and to do so faster and more effectively than potential adversaries. But even its most ardent advocates know that the West may never again be able to rely on its superior military technology. Robert Work, the deputy defence secretary who championed the third offset, argues that the West's most enduring military advantage will be the quality of the people produced by open societies. It would be comforting to think that the human factor, which has always been a vital component in past wars, will still count for something in the future. But there is uncertainty even about that.

Pride and prejudice

The odds on a conflict between the great powers

The great powers seem to have little appetite for full-scale war, but there is room for miscalculation

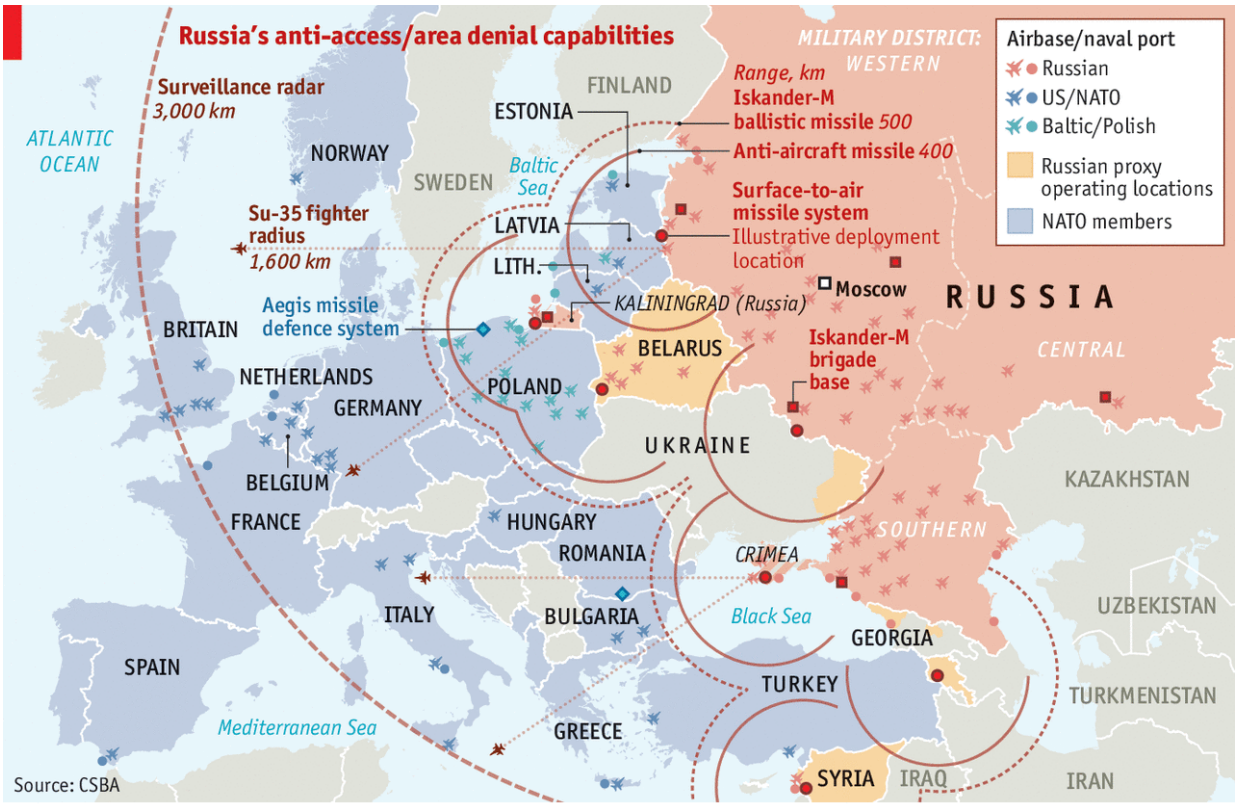
DESPITE THE EXTRAORDINARY decline in interstate wars over the past 70 years, many foreign-policy experts believe that the world is entering a new era in which they are becoming all too possible again. But there is a big difference between regional wars that might be triggered by the actions of a rogue state, such as North Korea or Iran, and those between great powers, which remain much less likely. Still, increased competition between America, Russia and China poses threats to the international order and does have a military dimension.

This special report will concentrate on what could lead to a future conflict between big powers rather than consider the threat of a war on the Korean peninsula, which is firmly in the present. A war to stop Iran acquiring nuclear weapons seems a more speculative prospect for now, but could become more likely a few years hence. Either would be terrible, but its destructive capacity would pale in comparison with full-blown conflict between the West and Russia or China, even if that did not escalate to a nuclear exchange.

The main reason why great-power warfare has become somewhat more plausible than at any time since the height of the cold war is that both Russia and China are dissatisfied powers determined to change the terms of a Western-devised, American-policed international order which they believe does not serve their legitimate interests. In the past decade both have invested heavily in modernising their armed forces in ways that exploit Western political and technical vulnerabilities and thwart America's ability to project power in what they see as their spheres of influence. Both have shown themselves prepared to impose their will on neighbours by force. Both countries' leaders are giving voice to popular yearning for renewed national power and international respect, and both are reaping the domestic political benefits. Where they differ is that Russia, demographically and economically, is a declining power with an opportunistic leadership, whereas China is clearly a rising one that has time on its side and sees itself as at least the equal of America, if not eventually its superior.

Russia's president, Vladimir Putin, wants to regain at least some of the prestige and clout his country lost after the collapse of the Soviet Union, an event he has described as the "greatest geopolitical tragedy of the [20th] century". He believes that in the 1990s the West rejected making Russia an equal partner, and that the European Union's and NATO's eastward expansion jeopardised Russia's external and internal security. In a statement on national-security strategy at the end of 2015 the Russian government designated NATO as the greatest threat it faced. It believes that the West actively tries to bring about "colour revolutions" of the sort seen in Ukraine, both in Russia's "near abroad" and in Russia itself.

Russia's armed forces, although no match for America's, are undergoing substantial modernisation, carry out frequent large-scale exercises and are capable of conducting high-intensity warfare at short notice across a narrow front against NATO forces. Russian military aircraft often probe European air defences and buzz NATO warships in the Baltic and the Black Sea, risking an incident that could rapidly get out of control.



Economist.com

War games carried out by the RAND Corporation, a think-tank, in 2015 concluded that in the face of a Russian attack "as currently postured, NATO cannot successfully defend the territory of its most exposed members". NATO has since slightly beefed up its presence in the Baltic states and Poland, but probably not enough to change the RAND report's conclusion that it would take Russian forces 60 hours at most to fight their way to the capital of Latvia or Estonia.

If that were to happen, NATO's political leaders would have to choose between three bad options: launch a bloody counter-offensive fraught with the risk of escalation; exacerbate the conflict itself by threatening targets in Russia; or concede defeat, with disastrous consequences for the alliance. Domestic support for the first and second options would be fragile (in Britain and Germany a Pew survey last year found only minority backing for NATO's Article 5 commitment to mutual defence if Russia were to attack a neighbouring alliance member, see chart). And Mr Putin's doctrine of "escalate to de-escalate" would almost certainly bring the threat, and possibly even the use, of Russian tactical nuclear weapons to encourage NATO to throw in the towel. Mr Putin reckons, probably correctly, that he has a much higher tolerance for risk than his Western counterparts.

The probability of such a direct test of NATO members' Article 5 promise is low. But Mr Putin has shown in Georgia, Ukraine and Syria that he is an opportunist prepared to roll the dice when he is feeling desperate or lucky. A second-term Trump administration, shorn of generals committed to NATO and with a more populist Republican party in Congress, might well tempt him, especially if low energy prices and a weak economy were creating mounting problems at home.

Up to a point

"Our country should use military force to defend a NATO ally if it got into a serious military conflict with Russia", % responding yes

Source: Pew Research Centre

Economist.com

Some suggest that America and China are destined to go to war, falling into the "Thucydides trap" as encountered in antiquity by Sparta and Athens. In essence, the established power feels threatened by the rising power, which in turn feels resentful and frustrated. Graham Allison, the author of a popular book expounding this thesis, believes that "war between the US and China in the decades ahead is not just possible, but much more likely than currently recognised."

Mr Allison's prognosis, based on an analysis of past conflicts between incumbent powers and thrusting newcomers, may be too deterministic. Although China and America do not have anything like the shared international agenda that America had with Britain when the roles were reversed, they are bound together by a web of economic interests. Strategic patience and taking the long view comes naturally to Chinese leaders, and successive American presidents (except perhaps the current one) have tried hard to show that far from wanting to keep China in its box, they wish to see it playing a full and responsible part in the international system. The previous contests for hegemony cited by Mr Allison were not conducted under the shadow of nuclear weapons, which for all their risks remain the ultimate disincentive for great powers to wage war against each other.

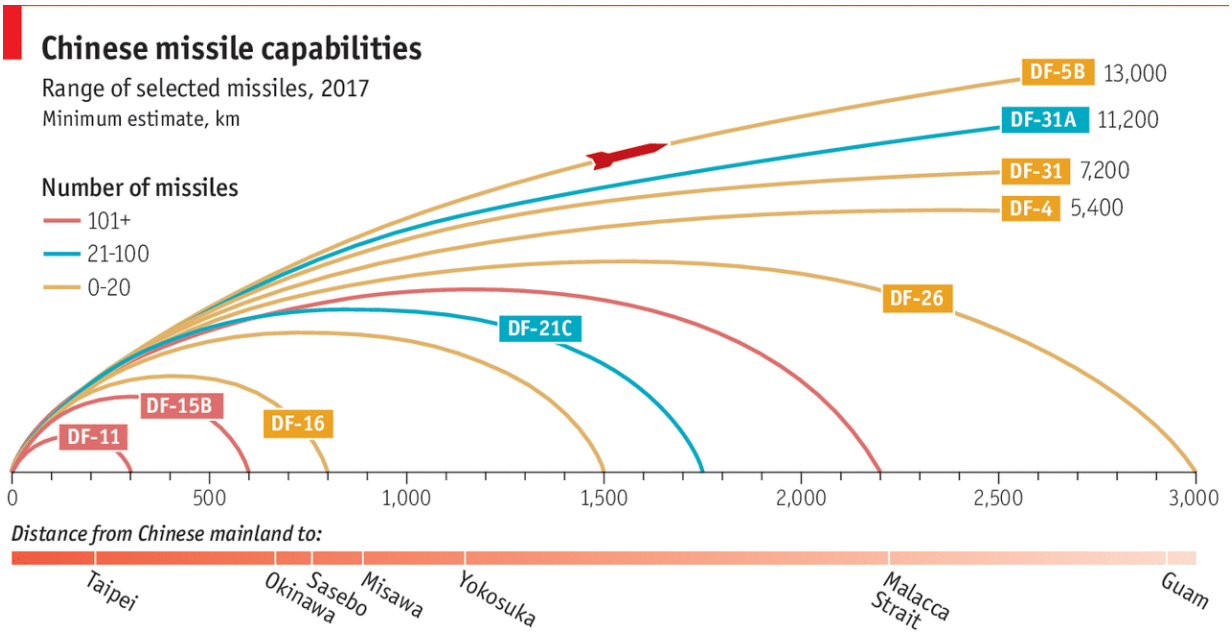
Moreover, says Jonathan Eyal of RUSI, a defence think-tank, demographic factors and changing social attitudes in China suggest that there would be little popular appetite for conflict with America, despite the sometimes nationalistic posturing of state media. Like other developed countries, the country has very low birth rates, fast-decreasing levels of violence and large middle classes who define success by tapping the latest smartphone or putting down a deposit on a new car. In a culture of coddling children prompted by the one-child policy, Chinese parents would probably be extremely reluctant to send their precious "snowflakes" off to war.

No coffins, please

Even in Russia, where Mr Putin has encouraged a revival of a more macho culture, he wants to avoid casualties as far as possible. In his view, the thousands of coffins returning from Afghanistan in the 1980s were partly to blame for the collapse of the Soviet Union, so he has gone to extraordinary lengths both to minimise and conceal the deaths of any conscripted troops in Ukraine. In Syria, he has used private military contractors wherever possible.

The risk that the West will run into a major conflict with China is lower than with Russia, but it is not negligible and may be growing. China resents the American naval presence in the western Pacific, and particularly the "freedom of navigation" operations that the US Seventh Fleet conducts in the South China Sea to demonstrate that America will not accept any Chinese claims or actions in the region that threaten its core national interests or those of its allies.

For its part, China is planning to develop its A2/AD capabilities, especially long-range anti-ship missiles and a powerful navy equipped with state-of-the-art surface vessels and a large submarine force. The idea is first to push the US Navy beyond the "first island chain" and ultimately make it too dangerous for it to operate within the "second island chain" (see map). Neither move is imminent, but China has already made a lot of progress. If there were a new crisis over Taiwan, America would no longer send an aircraft-carrier battle group through the Taiwan Strait to show its resolve, as it did in 1996.



Sources: US Department of Defence; United States-China Economic and Security Review Commission; MIIS; IISS
Economist.com

How such tensions will play out depends partly on America's allies. If Japan's recently re-elected prime minister, Shinzo Abe, succeeds in his ambition to change the country's pacifist constitution, the Japanese navy is likely to increase its capabilities and more explicitly train to fight alongside its American counterpart. At the same time other, weaker allies such as Vietnam, the Philippines, Malaysia and Indonesia may conclude that bowing to Chinese military and economic power is a safer bet than hoping for a declining America to fight their corner.

My truth against yours

Waging war with disinformation

The power of fake news and undue influence

THERE IS NOTHING new about either fake news or Russian disinformation campaigns. Back in 1983, at the height of the cold war, an extraordinary story appeared in a little-known pro-Soviet newspaper called the *Patriot*. It claimed to have evidence that the Pentagon had deliberately created AIDS as a biological weapon and was ready to export the virus to other countries, mainly in the developing world, as a way of gaining control over them. Within a few years the story had reappeared in mainstream publications in more than 50 countries.

In February last year, in the wake of revelations about Russia's interference in America's presidential election but before the full extent of its activities on Facebook, Twitter and Google had become known, the Russian defence minister, Sergei Shoigu, announced that he had created units within the army to wage an information war: "Essentially the information conflict is a component of general conflict. Deriving from that, Russia has made an effort to form structures that are engaged in this matter." He added that these were far more effective than anything Russia had used before for "counter-propaganda" purposes. A week earlier, General Petr Pavel, the Czech head of NATO's military committee, had revealed that a false report of a rape by German soldiers in Lithuania had been concocted by Russia.

The internet and social media are creating entirely new opportunities for influence operations (IO) and the mass manipulation of opinion. Those technologies allow IO accurately to target those people likely to be most susceptible to their message, taking advantage of the "echo-chamber" effect of platforms such as Facebook, where users see only news and opinions that confirm their prejudices.

Facebook now estimates that during and after the American election in 2016 a Russian-linked troll farm called the Internet Research Agency was responsible for at least 120 fake pages and 80,000 posts that were directly received by 29m Americans. Through sharing and liking, the number multiplied to nearly 150m, about two-thirds of the potential electorate. The ads aimed to exploit America's culture wars. Similar IO have been launched in Europe, where Russia attempts to bolster support for populist movements that oppose liberal social norms.

It is not just Russia that conducts IO against other countries. Jihadist extremists and hacker groups employed by rogue states or criminal networks pose similar if lesser threats. And although the big social-media companies now claim to be working on solutions, including better and quicker attribution of messages, Russian IO techniques are bound to adapt accordingly. Rand

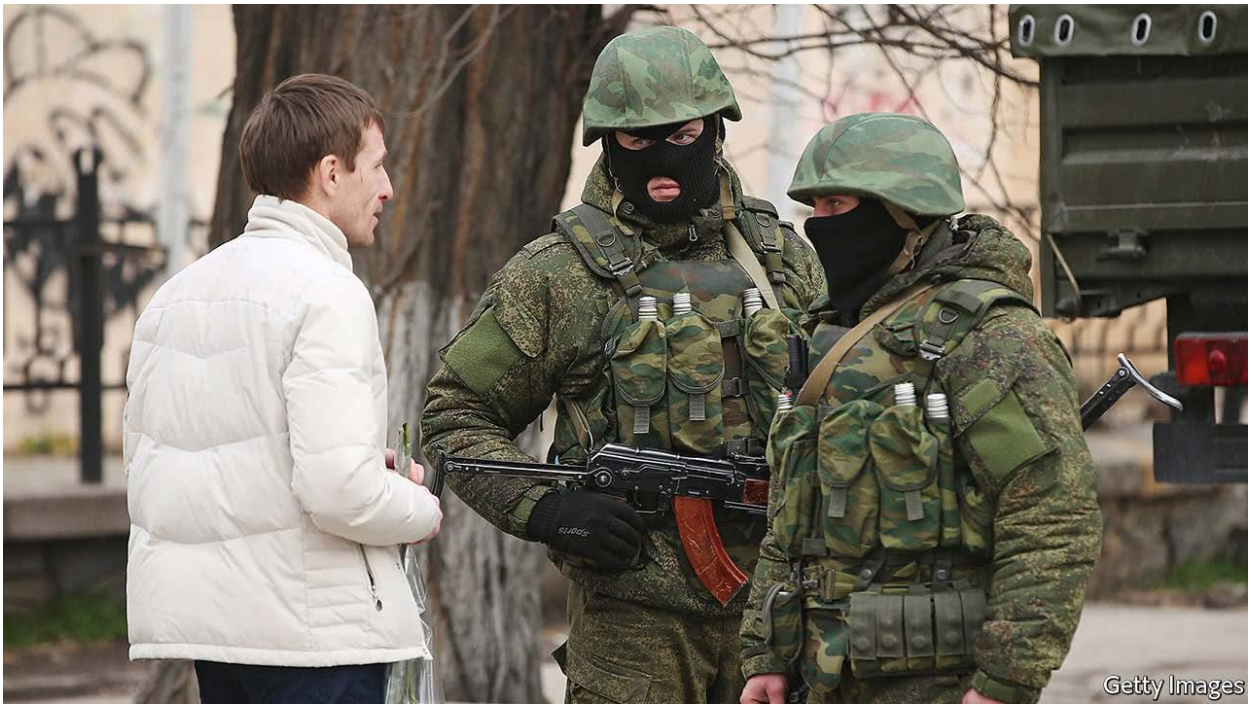
Waltzman, a former programme manager at America's Defence Advanced Research Projects Agency (DARPA) and now at the RAND Corporation, explains that "when target forces start to counter these [Russian] efforts and/or expose them on a large scale, the Russians are likely to accelerate the improvement of their techniques…in other words, an information-warfare arms race is likely to ensue."

In the future, "fake news" put together with the aid of artificial intelligence will be so realistic that even the best-resourced and most professional news organisation will be hard pressed to tell the difference between the real and the made-up sort. Official websites and social-media accounts will become increasingly vulnerable to hackers, who may be able not only to provoke stockmarket crashes and riots but even contrive crises between countries that may induce them to go to war with each other.

Shades of grey

Neither war nor peace

The uses of constructive ambiguity



A KEY ELEMENT of Chinese strategy is to "know your enemy". The generals who worked at the Academy of Military Science in Beijing studied every aspect of America's "revolution in military affairs" in the 1980s, driven by advances in microprocessors, sensors and communications. They concluded that although China was well placed to exploit the new

technologies to create its own version of “informationised” warfare, it would not be in a position to challenge American military might directly until the middle of the 21st century. To do so sooner would be suicidal. H.R. McMaster, Donald Trump’s national security adviser, once observed: “There are two ways to fight the United States: asymmetrically and stupid.”

Accordingly, the Chinese generals and their Russian counterparts, who had been equally impressed by the precision-strike capabilities that America demonstrated in the first Gulf war, sought ways to reap some of the political and territorial gains of military victory without crossing the threshold of overt warfare. They came up with the concept of a “grey zone” in which powers such as Russia, China and Iran can exercise aggression and coercion without exposing themselves to the risks of escalation and severe retribution. Mark Galeotti of the Institute of International Relations in Prague describes this approach as “guerrilla geopolitics”.

A key aspect of grey-zone challenges is that they should be sufficiently ambiguous to leave targets unsure how to respond. If they do too little, they will face a series of small but cumulatively significant defeats. If they do too much, they risk being held responsible for reckless escalation. As Hal Brands of the Philadelphia-based Foreign Policy Research Institute argues, grey-zone tactics are “frequently shrouded in misinformation and deception, and are often conducted in ways that are meant to make proper attribution of the responsible party difficult to nail down”. They are drawn from a comprehensive toolset that ranges from cyber attacks to propaganda and subversion, economic blackmail and sabotage, sponsorship of proxy forces and creeping military expansionism.

The clearest recent cases of grey-zone challenges are Russia’s intervention in Ukraine, China’s assertive behaviour in the South and East China Seas and Iran’s use of proxy militias to establish an arc of influence from Iraq through Syria into Lebanon. All three countries recognise and to some extent fear superior Western military power. But all of them also see vulnerabilities that they can exploit.

A Russian grey-zone strategy is to undermine faith in Western institutions and encourage populist movements by meddling in elections and using bots and trolls on social media to fan grievances and prejudice. The result, the Kremlin hopes, will sap the West’s capacity to respond resolutely to acts that defy international norms. If Russian cyber attacks did help to get Donald Trump elected, they have been astonishingly successful in their broader aim, if not in the narrower one of relieving Ukraine-related sanctions.

There is no evidence of Chinese complicity in Russian-style hacker attacks on the West, but officially sanctioned trolls send out hundreds of millions of social-media posts every year attacking Western values and pumping up nationalist sentiment. The advent of Mr Trump serves Chinese aims too. His repudiation of the Trans-Pacific Partnership removed a challenge to China’s regional economic hegemony, a key objective of its grey-zone strategy. And the American president’s hostility to free trade and his decision to withdraw from the Paris climate accord has allowed Xi Jinping to cast himself, improbably, as a defender of the international order.

As for Iran, America's inconsistency and lack of a long-term strategy in the Middle East has offered boundless opportunities for grey-zone advantage-seeking. Both George W. Bush and Barack Obama in their different ways allowed Iran to use a combination of soft religious and hard power through well-trained and equipped Shia militias to turn first Iraq and then most of Syria into something resembling Iranian satrapies.

Grey-zone success depends on patience and an ability to blend together all the instruments of state power in ways that pluralistic, democratic societies find harder to achieve. Hybrid warfare may be as old as warfare itself, but in Ukraine Russia provided a near-textbook example of it in its modern form, using a variety of techniques: sophisticated propaganda that stirred up local grievances and legitimised military action; cyber attacks on power grids and disruption of gas supplies; covert or deniable operations, such as sending "little green men" (soldiers in unmarked green army uniforms) into Crimea and providing weapons and military support to separatist irregular forces; the threat of "escalating to de-escalate", even including limited use of nuclear weapons. All this dissuaded the West from even contemplating a military response of any kind. Whenever the sale of defensive weapons to Ukraine was mooted in Washington, Mr Putin threatened to expand and intensify a war in which he claimed not to be a participant.

Russia's objective is not to "win" a war in Ukraine but to reverse the country's attempt to move out of Russia's orbit; to discourage other countries, such as Belarus, from trying anything similar; and to stoke nationalist and anti-Western sentiment at home. The effort has not been without cost. Sanctions have hurt. Making Crimea a viable entity will take time and lots of money. Most important of all, NATO has rediscovered some of its sense of purpose. But neither Mr Putin nor any likely successor would hesitate to apply the same hybrid-warfare techniques in the future should the need arise.

China's grey-zone campaign to assert uncontested control over the South China Sea and jurisdiction over disputed islands in the East China Sea has been going on for much longer, and has turned a darker shade of grey over time as the country's confidence and power has grown. Since 2009, when China submitted a map to the United Nations showing a "nine-dash line" that supported its claim to "indisputable sovereignty" over 90% of the South China Sea (see map), it has applied what James Holmes of the US Naval War College has described as "small-stick diplomacy" (as opposed to the big stick of conventional naval power), using its highly capable coastguard and militiamen embedded in its fishing fleet to push other littoral states out of waters to which it claims ancestral rights.

Economist.com

It has been able to cow most of its neighbours into sulky acquiescence while avoiding a direct confrontation with American naval ships, which did not want to risk a major incident over what China portrayed as maritime policing. When in 2013 China took its provocations a step further by sending civil engineers to the Spratly and Paracel archipelagoes to construct artificial islands, Xi Jinping said China had no intention of militarising them. But in 2017, satellite images released by the Centre for Strategic and International Studies showed shelters for missile batteries and military radar installations being constructed on the Fiery Cross, Mischief and Subi Reefs in the Spratly Islands. Fighter jets will be on their way next. Mr Holmes suggests that such strategic gains cannot now be reversed short of open warfare, which means they will almost certainly not be. Unlike traditional warfare, grey-zone strategies will not produce decisive results within a defined time frame. But both China and Russia have demonstrated that hybrid warfare, if not pushed too far, can achieve lasting, if not costless, results.

Hybrid warfare is hard to deter unless the target state itself resorts to hybrid strategies. Mr Brands sees no reason why America and its allies cannot play that game too. America has potent economic and financial tools at its disposal, along with an arsenal of cyber weapons, expert special forces, a network of alliances and unmatched soft power. But the West tends to think about conflict in a binary way: you are either at war or at peace; you win or you lose. Its adversaries are more attuned to conflict somewhere between war and peace, and to blurring distinctions between civil and military assets in pursuit of their goals. So for opponents of the rules-based system, the grey zone will remain fertile territory.

House to house

Preparing for more urban warfare

Much of the fighting in future wars is likely to take place in cities

DEEP IN THE southern Negev desert there is a small town called Baladia, with a main square, five mosques, cafés, a hospital, multi-storey blocks of flats, a kasbah and a cemetery. Oddly, it also has a number of well-constructed tunnels. The only people milling around in its streets are Israeli Defence Force (IDF) soldiers. Baladia, the Arab word for city, is part of the Tze'elim army base. It has been built to provide a realistic training ground for the next time the IDF is required to go into Gaza to destroy Hamas missile launchers.

Baladia is used not just by the IDF but by soldiers from other parts of the world too, including United Nations peacekeepers. Their interest reflects a growing, albeit reluctant, acceptance among Western armies that future fights are most likely to take place in cities. Megacities with populations of more than 10m are springing up across Africa and Asia. They are often ringed by closely packed slums controlled by neighbourhood gangs. Poor governance, high unemployment and criminality make them fertile territory for violent extremism.

It is hardly surprising that non-state adversaries of the West and its allies should seek asymmetric advantage by taking the fight into cities. Air power and precision-guided munitions lose some of their effectiveness in urban warfare because their targets can hide easily and have no scruples about using a densely packed civilian population as a shield.

Valuable lessons have been learned from the battle for Sadr City, a large suburb of Baghdad, in 2008, Israel going into Gaza in 2014 and the defeat of Islamic State (IS) in Mosul last year. Even with close air support, aerial surveillance and precision weapons supplied by Western allies, Iraqi security forces in Mosul (not to mention a civilian population held hostage by IS) took a terrible battering to defeat just a few thousand well-prepared insurgents. As General Mark Milley, the head of the US Army, puts it, "it took the infantry and the armour and the special operations commandos to go into that city, house by house, block by block, room by room…and it's taken quite a while to do it, and at high cost." He thinks that his force should now focus less on fighting in traditional environments such as woodland and desert and more on urban warfare.

To that end, he advocates smaller but well-armoured tanks that can negotiate city streets, and helicopters with a narrower rotor span that can fly between buildings. At the organisational level, that means operating with smaller, more compartmentalised fighting units with far more devolved decision-making powers.

General Milley and other military professionals are well aware that many of the emerging technologies will also be available to their adversaries. Today's smartphones provide encrypted communications that can befuddle Western forces' intelligence, surveillance and reconnaissance platforms. Quadcopter drones that can be bought from Amazon can send back live video of enemy positions. Commercially available unmanned ground vehicles can put improvised explosive devices in place.

Yet Western military forces should still enjoy a significant technological edge. They will have a huge range of kit, including tiny bird- or insect-like unmanned aerial vehicles that can hover outside buildings or find their way in. Unmanned ground vehicles can reduce the risk of resupplying troops in contested areas and provide medical evacuation for injured soldiers, and some of them will carry weapons. Worn-out or broken parts can be replaced near the front line thanks to 3D printing. A new generation of military vehicles will benefit from advances in solar energy and battery storage.

A key requirement will be for both direct and indirect fire to be highly discriminating. As General Milley says, "we can't go in there and just slaughter people." Part of the solution will be surveillance drones, along with more accurate small munitions. The Pentagon's DARPA research agency has come up with a "smart bullet" which cannot be dodged.

Commanders will also rely on artificial intelligence to analyse the vast amounts of data at their disposal almost instantly. Ben Barry of the International Institute for Strategic Studies says that big-data analytics will be able to provide a picture of the mood, morale and concerns of both combatants and civilians, which he thinks is at least as important as the military side.

For all the advances that new technologies can offer, General Milley says it is a fantasy to think that wars can now be won without blood and sacrifice: "After the shock and awe comes the march and fight…to impose your political will on the enemy requires you…to destroy that enemy up close with ground forces."

The greatest danger lies in miscalculation through a failure to understand an adversary's intentions, leading to an unplanned escalation that runs out of control. Competition in the "grey zone" between peace and war requires constant calibration that could all too easily be lost in the heat of the moment.

Stay well back

Using clever technology to keep enemies at bay

To counter regional challengers, America needs to regain its technological edge

A CRITICAL REASON for the success of Russia's and China's grey-zone strategies is that they have invested heavily in long-range sensor and precision-strike networks as well as cyber and space capabilities that can impose unacceptable costs on America projecting power in their regions. While America and its allies have spent much of the past 15 years fighting wars against irregular forces in the Middle East and Afghanistan, its adversaries have been studying the vulnerabilities in the Western way of warfare and exploiting technologies that have become cheaper and more readily available. They have also benefited from research and development passing from military institutions to the civil and commercial sectors.

Although at the strategic level American military power is still uncontested, its major adversaries' anti-access/area denial (A2/AD) investment has blunted its technology edge to such an extent that it can no longer count on local dominance in the early stages of a conflict. This means that America's adversaries are able to shelter low-intensity and paramilitary operations by carrying out small-scale but highly accurate attacks against American forces should they attempt to intervene on behalf of an ally.

It is doubtful that American commanders would recommend such a hazardous mission unless they were given the go-ahead to disable their opponents' A2/AD network (revealingly, the Chinese name for A2/AD is "counter-intervention"). That would require a major commitment of forces to strike targets inside Russian or Chinese territory, such as ground-to-air missile batteries and command, control, intelligence, surveillance and reconnaissance (C2ISR) nodes, which would probably result in heavy losses for the Americans. Even more important, such an operation would carry a risk so large as to make it infeasible. Even faced with the much less onerous task of suppressing Syrian air defences in 2012, Barack Obama was advised that 200-300 aircraft would be needed for an indefinite period.

Russia's growing A2/AD capability has received less attention than China's, but poses similar problems to America and its allies. NATO commanders fear that in the event of a crisis, missile systems in the Russian exclave of Kaliningrad and in western Russia itself could make the Baltic Sea a no-go area for its naval vessels. Similarly, albeit on a lesser scale, Iran can threaten shipping in the Gulf, including American carriers, and American air bases across the water.

Salami tactics

China's efforts are aimed mainly at degrading America's sea- and land-based air power and thus limiting the kind of war it can wage. The first step is to achieve what the Chinese call

“information dominance”. That means targeting America’s data and communications networks, especially in space. Physical attacks on satellites, including “blinding” them with lasers, would be combined with cyber attacks on computer systems.

To prevent America from operating close to China’s shore, a bristling arsenal of land-based air-defence and anti-ship missiles, along with fast missile boats, missile submarines and maritime strike aircraft, would attack US Navy vessels, as well as at US bases in Guam and Japan. In particular, China intends to push American carriers well beyond the unrefuelled range of their strike aircraft, such as the new F-35 stealth fighter, or risk catastrophic damage from anti-ship ballistic missiles.

The DF-21D, known as the “carrier killer”, is a ballistic missile that can travel by road. It has a range of over 1,000 miles and may carry manoeuvrable conventional warheads. It might or might not work as planned, but there is enough uncertainty to make it a powerful deterrent. At the same time China is building a strong blue-water navy with aircraft-carriers of its own, to which it is now adding heavily armed artificial islands in the South China Sea.

In response, the Pentagon in 2014 announced its “Third Offset Strategy”, concluding that if it could deter and defeat the “pacing threat” from China, it would be able to advance America’s interests and defend its allies not only in the Asia-Pacific region but anywhere in the world. The strategy focuses on areas such as autonomous learning systems, human-machine collaborative decision-making, assisted human operations, advanced manned-unmanned systems operations, networked autonomous weapons and high-speed projectiles, all of which are certain to have a major impact on the future of warfare.

The name could have been better chosen (and indeed, has been quietly dropped by the Trump administration). The first offset, in the 1950s, was America’s advantage in nuclear weapons as a way of repelling the Soviet Union’s much larger conventional forces if they were to attack Europe. The second, when the Soviets achieved nuclear parity, was the “look deep, strike deep” precision-guidance revolution of the 1980s, designed to achieve the same result without using nuclear weapons.

The third offset, like the second, aims to harness emerging technologies to restore America’s “overmatch” against near-peer adversaries, and thus its ability to project power even in highly contested environments. But whereas previous offsets secured a period of lasting technological advantage, even its most enthusiastic advocates (such as Bob Work, the deputy secretary of defence until 2017, who drove the effort for three years; or Michael O’Hanlon, a defence expert at the Brookings Institution) concede that this time America’s lead may be more fleeting.

One reason for caution is that the pace of innovation in many of the key enabling technologies, such as artificial intelligence, deep machine learning, robotics and autonomy, has accelerated. Another is that investment in research and development is being driven by the civil sector, which is looking for quick commercial rewards.

Russia, and particularly China, are both making AI a national priority, and have far fewer qualms than the West in how they go about it. According to Jim Lewis, an expert on the impact of

technology on warfare at CSIS, “when it comes to government data, the US doesn’t match what China collects on its citizens at all. They have a big sandbox to play in and a lot of toys and good people.” In China, where big data are bigger than anywhere else, privacy is not an issue, and there is no division between commercial research and military needs. By contrast, Google’s London-based DeepMind subsidiary, whose machine beat a grandmaster at the game of Go, refuses to work with the armed forces.

This is not to say that the effort to restore America’s technology edge will fail. It still spends nearly three times as much on defence as China does, and indeed more than all eight runners-up combined. Its forces have far more combat experience than any of their counterparts, and it has strengths in systems engineering that no other country can match. It continues to dominate commercial AI funding and has more firms working in the field than any other country.

More bang for the buck

But according to Bryan Clark of the Centre for Strategic and Budgetary Assessments, America’s chosen method of making a wide variety of investments and waiting to see what comes up fails to bring the most promising technologies to bear directly on the A2/AD challenge. In testimony to the Senate Armed Services Committee on the future of warfare, Mr Clark argued that America should apply new technologies to four main areas of warfare: undersea, strike, air and electromagnetic.

Quiet Chinese submarines and new active sonar systems are making it increasingly risky for American submarines to operate in Chinese coastal waters. Small, hard-to-detect unmanned undersea vehicles (UUVs) could be used to clear mines, hunt enemy submarines in shallow waters and gather intelligence. Larger ones could deploy seabed payloads such as long-endurance sensors, power packs for other UUVs and extra missiles for manned submarines.

In the air, America may try to degrade an adversary’s integrated air-defence systems (IADs) by interfering with their sensors and control systems, then send out networked swarms of small unmanned aerial vehicles (UAVs) to inflict further damage before deploying penetrating long-range stealth bombers such as the B2 and the new B21. But air supremacy of the kind it has enjoyed since the end of the cold war may be passing. To achieve even local dominance, it will need longer-range sensors and lasers to detect enemy aircraft. Manned aircraft will increasingly be platforms for sensors, data-gathering and stand-off missiles.

Dominance of the electromagnetic spectrum will become more and more important. New ways of achieving it will include stealth technologies to conceal the radar signature of ships and planes; protecting space-based communications networks from attack; launching decoys; and defences against incoming missile salvoes. For example, miniaturised electromagnetic weapons (EMW) mounted on swarms of expendable UAVs launched close to shore from a large UUV could jam an opponent’s targeting sensors and communications. Electromagnetic rail guns mounted on ships, which can fire projectiles at 4,500 miles an hour to the edge of space, could counter ballistic-missile warheads.

The Pentagon's lumbering acquisition system will find it hard to accommodate any of this. To get even close to keeping up with the pace of innovation, says Mr Work, it will have to move to rapid prototyping and adopt a different attitude to testing, emulating Silicon Valley's readiness to "fail fast". It will also have to find less bureaucratic ways of doing business with firms developing key technologies. To that end, the Pentagon has established DIUx (Defence Innovation Unit Experimental) to team up with companies that would not previously have worked with it.

Finding the money will be another problem. And whereas the second offset was underwritten by the commitment of successive administrations, the third offset is no longer considered a strategy, merely a helpful way to tackle wider defence modernisation. Above all, it needs a compelling operational concept, tested in war games, that service chiefs feel able to support. The Chinese and the Russians will be watching with interest.

Not so MAD

Why nuclear stability is under threat

Mutually assured destruction has served as the ultimate deterrent, but for how much longer?

NUCLEAR WEAPONS, LIKE the poor, seem likely always to be with us. Even though arms-control agreements between America and the Soviet Union, and then Russia, have drastically

reduced overall numbers, both countries are committed to costly long-term modernisation programmes for their strategic nuclear forces that should ensure their viability for the rest of the century.

Russia is about halfway through recapitalising its strategic forces, which include a soon-to-be-deployed road-mobile intercontinental ballistic missile (ICBM); a new heavy ICBM; eight new ballistic-missile submarines (SSBNs), most of which will be in service by 2020; upgraded heavy bombers; and a new stealth bomber able to carry hypersonic cruise missiles. America will replace every leg of its nuclear triad over the next 30 years, at an estimated cost of $1.2trn. There will be 12 new SSBNs; a new penetrating strike bomber, the B21; a replacement for the Minuteman III ICBMs; and a new long-range air-launched cruise missile. As Tom Plant, a nuclear expert at RUSI, a think-tank, puts it: “For both Russia and the US, nukes have retained their primacy. You only have to look at how they are spending their money.”

Other states with nuclear weapons, such as China, Pakistan, India and, particularly, North Korea, are hard at work to improve both the quality and the size of their nuclear forces. Iran’s long-term intentions remain ambiguous, despite the deal in 2015 to constrain its nuclear programme. Nuclear weapons have lost none of their allure or their unique ability to inspire dread. Whether or not they are ever used in anger, they are very much part of the future of warfare.

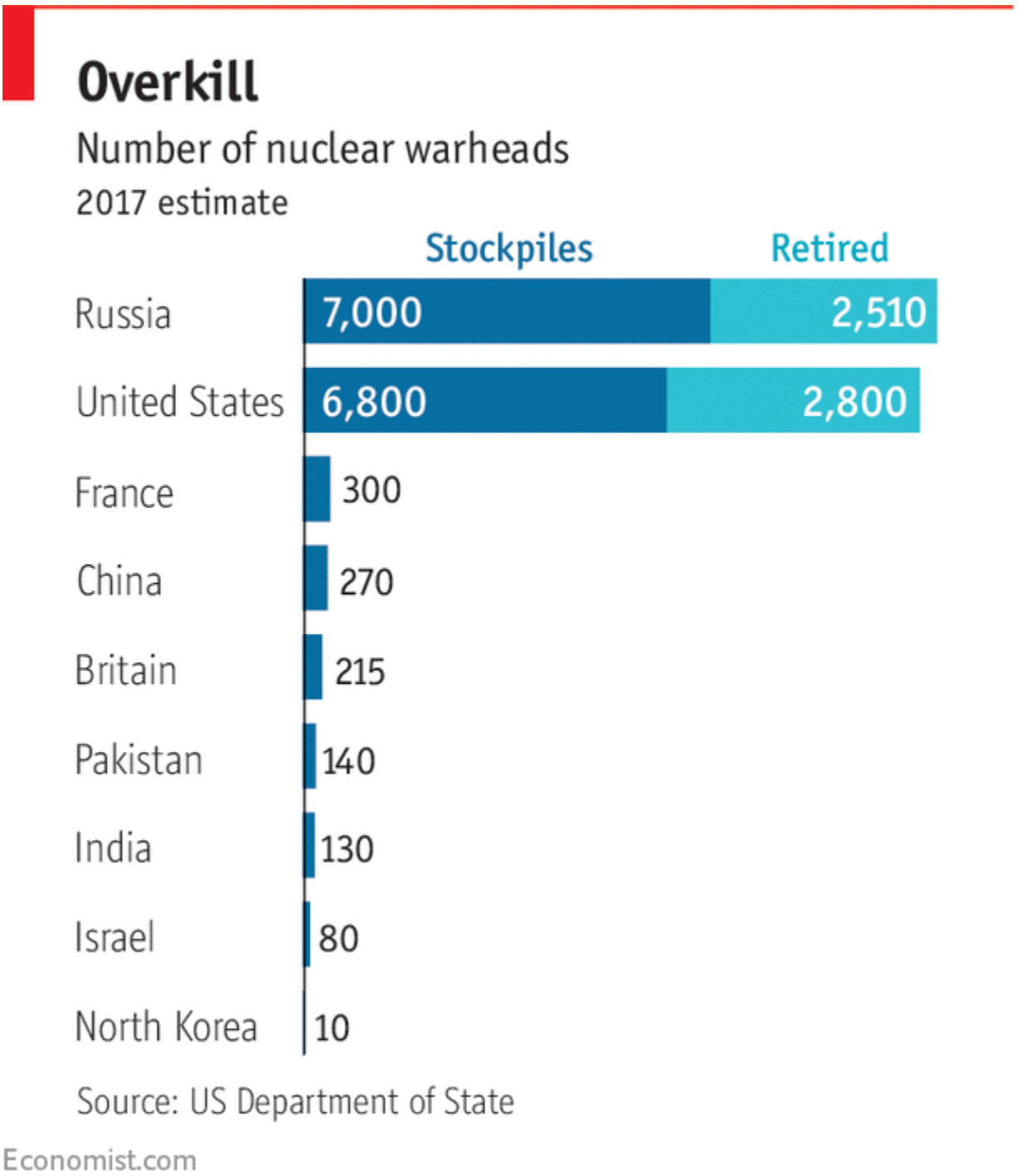
So far, the best argument for nuclear weapons has been that the fear of mutually assured destruction (MAD) has deterred states that possess them from going to war with each other. MAD rests on the principle of a secure second-strike capability, which means that even if one side is subjected to the most wide-ranging first strike conceivable, it will still have more than enough nuclear weapons left to destroy the aggressor. When warheads became accurate enough to obliterate most of an adversary’s missiles in their silos, America and Russia turned to submarines and mobile launchers to keep MAD viable.

A more dangerous world

It still is, and is likely to remain so for some time. But disruptive new technologies, worsening relations between Russia and America and a less cautious Russian leadership than in the cold war have raised fears that a new era of strategic instability may be approaching. James Miller, who was under-secretary of defence for policy at the Pentagon until 2014, thinks that the deployment of increasingly advanced cyber, space, missile-defence, long-range conventional strike and autonomous systems “has the potential to threaten both sides’ nuclear retaliatory strike capabilities, particularly their command-and-control apparatuses”, and that “the potential of a dispute leading to a crisis, of a crisis leading to a war, and of a war escalating rapidly” is growing.

In a new report, Mr Miller and Richard Fontaine, the president of the Centre for a New American Security (CNAS), identify cyber and counter-space (eg, satellite jammers, lasers and high-power microwave-gun systems) attacks as possible triggers for an unplanned conflict. Other new weapons may threaten either side’s capability for nuclear retaliation, particularly their strategic command-and-control centres. James Acton, a nuclear-policy expert at the Carnegie Endowment for International Peace, lists three trends that could undermine stability in a future crisis:

advanced technology that can threaten the survivability of nuclear attacks; command-and-control systems that are used for both nuclear and conventional weapons, leaving room for confusion; and an increased risk of cyber attacks on such systems because of digitisation.



Both America and Russia rely heavily on digital networks and space-based systems for command, control, communications, intelligence, surveillance and reconnaissance (C3ISR) to run almost every aspect of their respective military enterprises. Cyber space and outer space therefore offer attackers tempting targets in the very early stages of a conflict. In the utmost secrecy, both sides have invested heavily in offensive cyber capabilities. In 2013 the Defence Science Board advised the Pentagon that: "The benefits to an attacker using cyber exploits are potentially spectacular. Should the United States find itself in a full-scale conflict with a peer adversary, attacks would be expected to include denial of service, data corruption, supply-chain corruption, traitorous insiders, kinetic and related non-kinetic attacks at all altitudes from under water to space. US guns, missiles and bombs may not fire, or may be directed against our own troops. Resupply, including food, water, ammunition and fuel, may not arrive when or where needed. Military commanders may rapidly lose trust in the information and ability to control US systems and forces."

One problem with this is that the space architecture on which America depends for its nuclear command and control, including missile early warning, is also used for conventional warfare. That means a conventional attack might be mistaken for a pre-emptive nuclear strike, which could lead to rapid escalation. Another difficulty is that an aggressor may be tempted to go after cyber and space assets in the hope of causing major damage to a target's defences without actually killing anybody. That would raise doubts over whether nuclear retaliation could be justified. A third worry is that because of the potential speed and surprise of such attacks, some responses might be delegated to autonomous systems that can react in milliseconds. Lastly, there is the possibility of "false flag" cyber operation by a rogue state or non-state hacker group.

Don't worry just yet

For now, the prospects of a successful disarming strike remain sufficiently remote to leave the strategic balance intact. Mr Miller argues that it would require a "fundamental transformation in the military-technological balance…enabled by the development and integration of novel military capabilities" to upset the balance.

Ominously, he thinks that such a fundamental transformation may now be on the horizon, in the shape of conventional prompt global strike (CPGS) and new missile-defence systems. Both China and Russia fear that new American long-range non-nuclear strike capabilities could be used to deliver a disarming attack on a substantial part of their strategic forces or decapitate their nuclear command and control. Although they would still launch their surviving nuclear missiles, improved missile-defence systems would mop up most of the remainder before their warheads could do any damage.

Still, Michael Elleman, a missile expert at the International Institute for Strategic Studies, reckons that for now those concerns are overblown. As much as anything, he says, they are talked up to restrain investment in the enabling technologies: "They [the Russians and the Chinese] are saying to the US, the trouble with you guys is that you never know when to stop."

CPGS would involve a hypersonic missile at least five times faster than the speed of sound and a range of more than 1,000 miles. This could be achieved in several ways. One would be to stick a

conventional warhead on an ICBM or a submarine-launched ballistic missile—a cheap solution but a dangerous one, because defenders would not know whether they were under conventional or nuclear attack, so they might overreact.

The alternatives would be a cruise missile powered by a rocket-boosted scramjet (a supersonic combusting ramjet) engine, or a boost-glide vehicle that would be launched from a ballistic missile and then fly towards its target like a paper dart. Glide vehicles pull up after re-entering the atmosphere, using the curvature of the Earth to delay detection by ballistic-missile defences. Both types would be manoeuvrable, and would be accurate to within a few metres of their target. However, they, too, could carry nuclear warheads, again leaving the target uncertain what kind of attack it was under. America first tested a glide vehicle in 2010, but seems in no rush to deploy them. Russia and China have more recently tested hypersonic glide missiles.

Current American missile-defence systems, such as Patriot, THAAD (terminal high-altitude area defence) and Aegis, provide quite effective regional defence but are not designed to cope with a salvo of ICBMs. The Ground-based Midcourse Defence system in Alaska and California is supposed to provide some defence of the homeland against a few missiles launched by a North Korea or an Iran, but it was never designed to defeat a massive salvo attack by a major adversary.

However, substantial improvements are on their way. Mr Elleman describes the SM-3 IIA interceptors, which could be deployed as soon as next year on Aegis-class destroyers, as a “big deal”. They are much faster than their predecessors, and Mr Miller thinks that if hundreds of them were put on ships close to America, they might support a late midcourse defence against Russian ICBMs.

More exotic missile defences are not far behind. Mr Elleman says that in about five years’ time it may be possible to put solid-state lasers on large numbers of unmanned aerial vehicles (UAVs) orbiting at very high altitude. Small missiles could also be put on UAVs as boost-phase interceptors, firing a minute or so after launch. Interception at that stage is technically much easier than later on because the target is much larger when all its stages are still intact, and moving more slowly.

Mr Elleman believes that for now the advantage is likely to remain with the attacker rather than the defender, but like Mr Miller he fears that emerging technologies could “undermine crisis stability very rapidly”. Yet if arms-control agreements could be reached at the height of the cold war, it should surely be possible for America, Russia and China to talk to each other now to avoid persistent instability.

War at hyperspeed

Getting to grips with military robotics

Autonomous robots and swarms will change the nature of warfare

PETER SINGER, AN expert on future warfare at the New America think-tank, is in no doubt. “What we have is a series of technologies that change the game. They’re not science fiction. They raise new questions. What’s possible? What’s proper?” Mr Singer is talking about artificial intelligence, machine learning, robotics and big-data analytics. Together they will produce systems and weapons with varying degrees of autonomy, from being able to work under human supervision to “thinking” for themselves. The most decisive factor on the battlefield of the future may be the quality of each side’s algorithms. Combat may speed up so much that humans can no longer keep up.

Frank Hoffman, a fellow of the National Defence University who coined the term “hybrid warfare”, believes that these new technologies have the potential not just to change the character of war but even possibly its supposedly immutable nature as a contest of wills. For the first time, the human factors that have defined success in war, “will, fear, decision-making and even the human spark of genius, may be less evident,” he says.

Weapons with a limited degree of autonomy are not new. In 1943 Germany produced a torpedo with an acoustic homing device that helped it find its way to its target. Tomahawk cruise missiles, once fired, can adjust their course using a digital map of Earth’s contours. Anti-missile

systems are pre-programmed to decide when to fire and engage an incoming target because the human brain cannot react fast enough.

But the kinds of autonomy on the horizon are different. A report by the Pentagon's Defence Science Board in 2016 said that "to be autonomous, a system must have the capability to independently compose and select among different courses of action to accomplish goals based on its knowledge and understanding of the world, itself, and the situation." What distinguishes autonomous systems from what may more accurately be described as computerised automatic systems is that they work things out as they go, making guesses about the best way to meet their targets based on data input from sensors. In a paper for the Royal Institute of International Affairs in London, Mary Cummings of Duke University says that an autonomous system perceives the world through its sensors and reconstructs it to give its computer "brain" a model of the world which it can use to make decisions. The key to effective autonomous systems is "the fidelity of the world model and the timeliness of its updates".

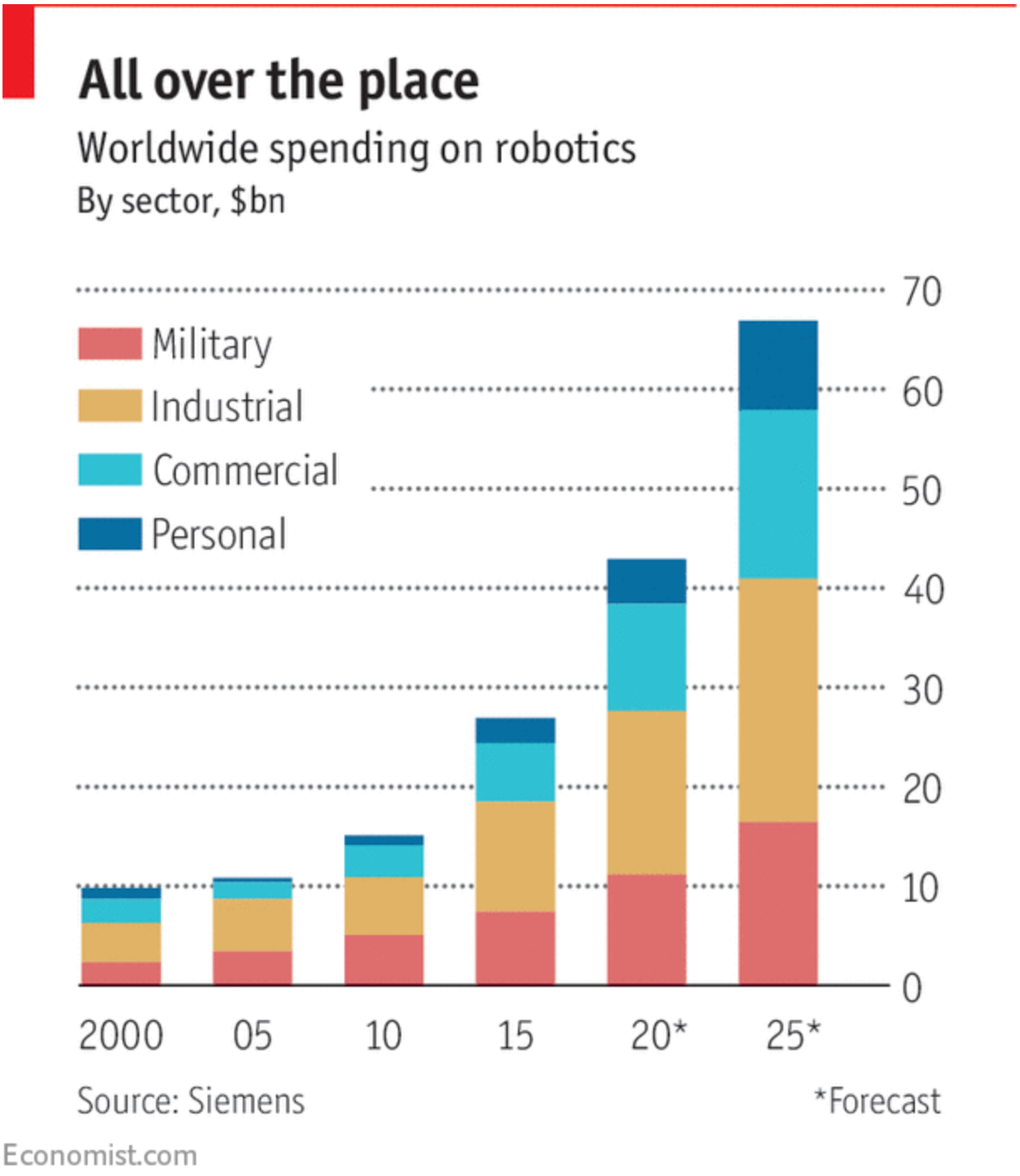
A distinction needs to be made between "narrow" AI, which allows a machine to carry out a specific task much better than a human could, and "general" AI, which has far broader applications. Narrow AI is already in wide use for civilian tasks such as search and translation, spam filters, autonomous vehicles, high-frequency stock trading and chess-playing computers.

Waiting for the singularity

General AI may still be at least 20 years off. A general AI machine should be able to carry out almost any intellectual task that a human is capable of. It will have the ability to reason, plan, solve problems, think abstractly and learn quickly from experience. The AlphaGo Zero machine which last year learned to play Go, the ancient strategy board game, was hailed as a major step towards creating the kind of general-purpose algorithms that will power truly intelligent machines. By playing millions of games against itself over 40 days it discovered strategies that humans had developed over thousands of years, and added some of its own that showed creativity and intuition.

Mankind is still a long way from the "singularity", the term coined by Vernor Vinge, a science-fiction writer, for the moment when machines become more intelligent than their creators. But the possibility of killer robots can no longer be dismissed. Stephen Hawking, Elon Musk, Bill Gates and many other experts believe that, handled badly, general AI could be an existential threat to the human race.

In the meantime, military applications of narrow AI are already close to bringing about another revolution. Robert Work, the architect of America's third offset strategy, stresses that this is not all about autonomous drones, important though they will increasingly become. His main focus has been on human-machine collaboration to help humans make better decisions much faster, and "combat teaming", using unmanned and manned systems together.



Autonomous systems will draw on machine deep learning to operate “at the speed of light” where humans cannot respond fast enough to events like cyber attacks, missiles flying at hypersonic speed or electronic warfare. AI will also become ever more important in big-data analytics. Military analysts are currently overwhelmed by the amount of data, especially video, being generated by surveillance drones and the monitoring of social-media posts by terrorist groups. Before leaving the Pentagon, Mr Work set up an algorithmic-warfare team to consider how AI can help hunt Islamic State fighters in Syria and mobile missile launchers in North

Korea. Cyber warfare, in particular, is likely to become a contest between algorithms as AI systems look for network vulnerabilities to attack, and counter-autonomy software learns from attacks to design the best response.

In advanced human-machine combat teaming, UAVs will fly ahead of and alongside piloted aircraft such as the F-35. The human pilot will give the UAV its general mission instructions and define the goal, such as striking a particular target, but the UAV will be able to determine how it meets that goal by selecting from a predefined set of actions, and will respond to any unexpected challenges or opportunities. Or unmanned ground vehicles might work alongside special forces equipped with wearable electronics and exoskeletons to provide machine strength and protection. As Mr Work puts it: “Ten years from now, if the first through a breach isn’t a fricking robot, shame on us.”

Autonomous “uninhabited” vehicles, whether in the air, on the ground or under the sea, offer many advantages over their manned equivalents. Apart from saving money on staff, they can often be bolder and more persistent than humans because they do not get tired, frightened, bored or angry. They are also likely to be cheaper and smaller than manned versions because they do not have to protect people from enemy attack, so they can be deployed in greater numbers and in more dangerous situations.

Increasingly autonomous drones will be able to perform a range of tasks that will soon make them indispensable. UAVs will carry out the whole range of reconnaissance or strike missions, and stealth variants will become the tip of the spear for penetrating sophisticated air defences. Some will be designed to loiter at altitude while waiting for a target to emerge. Israel already deploys the Harop, an autonomous anti-radiation drone which can fly for up to six hours, attacking only when an enemy air-defence radar lights up. Autonomous high-altitude UAVs will be used as back-up data links in case satellites are destroyed, or as platforms for anti-missile solid-state lasers. Larger UAVs will be deployed as tankers and transport aircraft that can operate close to the action.

Underwater warfare will become ever more important in the future because the sea offers a degree of sanctuary from which power can be projected within A2/AD zones. Unmanned undersea vehicles (UUVs) will be able to carry out a wide range of difficult and dangerous missions, such as mine clearance or mine-laying near an adversary’s coast; distributing and collecting data from undersea anti-submarine sensor networks in contested waters; patrolling with active sonar; resupplying missiles to manned submarines; and even becoming missile platforms themselves, at a small fraction of the cost of nuclear-powered attack submarines. There are still technical difficulties to be overcome, but progress is accelerating.

Potentially the biggest change to the way wars are fought will come from deploying lots of robots simultaneously. Paul Scharre, an autonomous-weapons expert at CNAS who has pioneered the concept of “swarming”, argues that “collectively, swarms of robotic systems have the potential for even more dramatic, disruptive change to military operations.” Swarms can bring greater mass, co-ordination, intelligence and speed.

The many, not the few

As Mr Scharre points out, swarming will solve a big problem for America. The country currently depends on an ever-decreasing number of extremely capable but eye-wateringly expensive multi-mission platforms which, if lost at the outset of a conflict, would be impossible to replace. A single F-35 aircraft can cost well over $100m, an attack submarine $2.7bn and a Ford-class carrier with all its aircraft approaching $20bn.

By contrast, low-cost, expendable distributed platforms can be built in large numbers and controlled by relatively few humans. Swarms can make life very difficult for adversaries. They will come in many shapes and sizes, each designed to carry out a particular mission, such as reconnaissance over a wide area, defending ships or troops on the ground and so on. They will be able to work out the best way to accomplish their mission as it unfolds, and might also be networked together into a single "swarmanoid". Tiny 3D-printed drones, costing perhaps as little as a dollar each, says Mr Scharre, could be formed into "smart clouds" that might permeate a building or be air-dropped over a wide area to look for hidden enemy forces.

It is certain that autonomous weapons systems will appear on the battlefield in the years ahead. What is less clear is whether America will be the first to deploy them. In July 2017 China produced its "Next-Generation Artificial-Intelligence Development Plan", which designates AI as the transformative technology underpinning future economic and military power. It aims for China to become the pre-eminent force in AI by 2030, using a strategy of "military-civil fusion" that America would find hard to replicate. And in September Vladimir Putin told Russian children returning to school that "artificial intelligence is the future, not only for Russia but for all of mankind…whoever becomes the leader in this sphere will become the ruler of the world." Elon Musk, of Tesla and SpaceX fame, responded by tweeting that "competition for AI superiority at national level [is the] most likely cause of WW3."

Peter Singer is less apocalyptic than Mr Musk, but he agrees that the competition for AI dominance is fuelling an arms race that will itself generate insecurity. This arms race may be especially destabilising because the capabilities of robotic weapons systems will not become clear until someone is tempted to use them. The big question is whether this competition can be contained, and whether rules to ensure human control over autonomous systems are possible—let alone enforceable.

Man and machine

Autonomous weapons are a game-changer

AI-empowered robots pose entirely new dangers, possibly of an existential kind

MANY OF THE trends in warfare that this special report has identified, although worrying, are at least within human experience. Great-power competition may be making a comeback. The attempt of revisionist powers to achieve their ends by using hybrid warfare in the grey zone is taking new forms. But there is nothing new about big countries bending smaller neighbours to their will without invading them. The prospect of nascent technologies contributing to instability between nuclear-armed adversaries is not reassuring, but past arms-control agreements suggest possible ways of reducing the risk of escalation.

The fast-approaching revolution in military robotics is in a different league. It poses daunting ethical, legal, policy and practical problems, potentially creating dangers of an entirely new and, some think, existential kind. Concern has been growing for some time. Discussions about lethal autonomous weapons (LAWs) have been held at the UN's Convention on Certain Conventional Weapons (CCW), which prohibits or restricts some weapons deemed to cause unjustifiable suffering. A meeting of the CCW in November brought together a group of government experts and NGOs from the Campaign to Stop Killer Robots, which wants a legally binding international treaty banning LAWs, just as cluster munitions, landmines and blinding lasers have been banned in the past.

Most people agree that when lethal force is used, humans should be involved. But what sort of human control is appropriate?

The trouble is that autonomous weapons range all the way from missiles capable of selective targeting to learning machines with the cognitive skills to decide whom, when and how to fight. Most people agree that when lethal force is used, humans should be involved in initiating it. But determining what sort of human control might be appropriate is trickier, and the technology is moving so fast that it is leaving international diplomacy behind.

To complicate matters, the most dramatic advances in AI and autonomous machines are being made by private firms with commercial motives. Even if agreement on banning military robots could be reached, the technology enabling autonomous weapons will be both pervasive and easily transferable.

Moreover, governments have a duty to keep their citizens secure. Concluding that they can manage quite well without chemical weapons or cluster bombs is one thing. Allowing potential adversaries a monopoly on technologies that could enable them to launch a crushing attack because some campaign groups have raised concerns is quite another.

As Peter Singer notes, the AI arms race is propelled by unstoppable forces: geopolitical competition, science pushing at the frontiers of knowledge, and profit-seeking technology businesses. So the question is whether and how some of its more disturbing aspects can be constrained. At its simplest, most people are appalled by the idea of thinking machines being allowed to make their own choices about killing human beings. And although the ultimate nightmare of a robot uprising in which machines take a genocidal dislike to the human race is still science fiction, other fears have substance.

Nightmare scenarios

Paul Scharre is concerned that autonomous systems might malfunction, perhaps because of badly written code or because of a cyber attack by an adversary. That could cause fratricidal attacks on their own side's human forces or escalation so rapid that humans would not be able to respond. Testing autonomous weapons for reliability is tricky. Thinking machines may do things in ways that their human controllers never envisaged.

Much of the discussion about "teaming" with robotic systems revolves around humans' place in the "observe, orient, decide, act" (OODA) decision-making loop. The operator of a remotely piloted armed Reaper drone is in the OODA loop because he decides where it goes and what it does when it gets there. An on-the-loop system, by contrast, will carry out most of its mission without a human operator, but a human can intercede at any time, for example by aborting the mission if the target has changed. A fully autonomous system, in which the human operator merely presses the start button, has responsibility for carrying through every part of the mission, including target selection, so it is off the loop. An on-the-loop driver of an autonomous car would let it do most of the work but would be ready to resume control should the need arise. Yet if the car merely had its destination chosen by the user and travelled there without any further intervention, the human would be off the loop.

For now, Western armed forces are determined to keep humans either in or on the loop. In 2012 the Pentagon issued a policy directive: "These [autonomous] systems shall be designed to allow

commanders and operators to exercise appropriate levels of human judgment over the use of force. Persons who authorise the use of, direct the use of, or operate, these systems must do so with appropriate care and in accordance with the law of war, applicable treaties, weapons-systems safety rules and applicable rules of engagement."

That remains the policy. But James Miller, the former under-secretary of Defence for Policy at the Pentagon, says that although America will try to keep a human in or on the loop, adversaries may not. They might, for example, decide on pre-delegated decision-making at hyper-speed if their command-and-control nodes are attacked. Russia is believed to operate a "dead hand" that will automatically launch its nuclear missiles if its seismic, light, radioactivity and pressure sensors detect a nuclear attack.

Mr Miller thinks that if autonomous systems are operating in highly contested space, the temptation to let the machine take over will become overwhelming: "Someone will cross the line of sensibility and morality." And when they do, others will surely follow. Nothing is more certain about the future of warfare than that technological possibilities will always shape the struggle for advantage.