TONY BLAIR
INSTITUTE
FOR GLOBAL
CHANGE

Ukraine: A Wake-Up Call for the West on Defence

JACOB DELORME
MELANIE GARSON
JEEGAR KAKKAD
NATHAN LLOYD
RORY MACLEOD
BRIANNA MILLER
RUBY OSMAN
NILS PETERSON
DANIEL SLEAT
HARRY SUMMERS

Contents

Published at https://institute.global/policy/ukraine-wake-call-west-defence on March 15 2022

Overview

Russia's invasion of Ukraine, for all its apparent difficulties on the ground, has shown that the West faces a more assertive Russia that is willing to use its military capability. China too has been investing heavily in defence, and while we can hope that Beijing is less antagonistic than Moscow, we should be fully prepared for all possible threats.

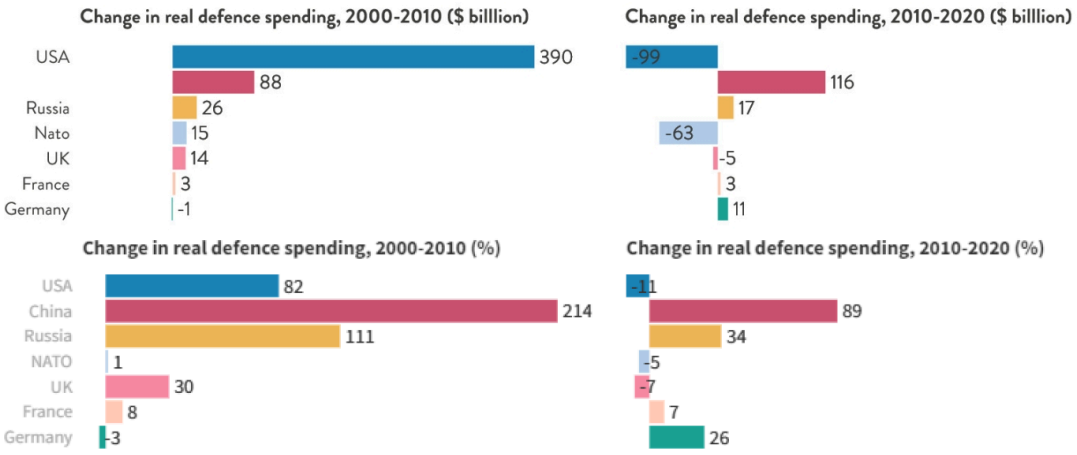
Ukraine is a wake-up call for the West. We need to rethink our collective approach to defence spending and capabilities, and consider enhanced cooperation – or else, risk the values we believe in eroding.

This is more than just a question of spending, but finance does matter. French military spending has increased by 15 per cent since 2000, the UK's defence spending by 20 per cent, Germany's by 22 per cent and the US's by 61 per cent. [1] In comparison, China's has increased by 495 per cent and Russia's by 183 per cent. Between 2010 and 2020, the increase in Russian defence spending was 43 per cent higher than the equivalent for Western Europe combined. [2]

How the money is deployed is also important. We need to address the shifting nature of conflict, particularly the rise of grey-zone activity: competitive interactions among and between non-state actors that fall below the threshold for war but disrupt the peace. [3] Ranging from cyber-attacks, disinformation and electoral interference to economic coercion and strategic investments, this activity, enabled by technologies, favours authoritarian states with a close nexus to their citizens and private sector. These states are able to leverage their centralised capabilities to exploit cracks in Western democracies.

It is clear that Western countries need a new plan, but it must be more than a kneejerk reaction that simply focuses on spending big on hard power in response to Putin's invasion. Instead, smarter spending should be underpinned by a forward-thinking strategy that looks critically at the different challenges posed by different actors, and which is willing to draw on the full range of hard- and soft-power levers at our disposal to protect and promote liberal values.

Figure 1 – Changes in real defence spending, 2000-2010 and 2010-2020, in constant $ billions and by percentage



Source: TBI and SIPRI

The Russia–Ukraine War: A Wake–Up Call

Russia's invasion of Ukraine has highlighted how Western militaries are struggling to reframe their strategic objectives, operations (for instance, how they would actually fight in the future), and investments in technology, training and acquisition.

Putin's decision to invade Ukraine was no doubt buoyed by the perception of a divided and weaker West. The way in which the US blindsided its allies with the Afghanistan withdrawal in 2021 contrasted starkly with the shrewd diplomacy that had helped to assemble the coalition that entered the country 20 years ago. Since then, a previously united Western alliance has seemingly become fractured – more vulnerable to the individualistic pull of national politics, and much less interested in the concept of institutions that bind the West together, such as NATO and the EU.

Putin's assessment may well have been accurate, but his assumption that Russia's invasion of Ukraine would not reverse this course was way off the mark. In a demonstration of strength and unity, the West has banded together to form a powerful front – but this can only hold firm so long as the alliance continues to work together on global-security issues and in defence of liberal democratic values.

This rejuvenated Western alliance must not only consider whether its military forces are on a trajectory for remaining a step ahead of the Russians and Chinese, it must also refresh the structures and frameworks through which it makes collective policy decisions on issues of diplomacy, defence and security.

The withdrawal from Afghanistan, planned scale downs of Western forces in conflict-affected regions such as the Sahel, lukewarm engagement in Libya and a reluctance to follow through on promises to stand against the use of chemical and biological weapons in Syria all point to a broader pivot away from engagement. In its place, Western countries have rightly begun to prioritise soft-power foreign-policy levers; where they do engage militarily, they have demonstrated a preference for over-the-horizon capabilities. However, the West should remain wary of creating hard-power vacuums that authoritarian states look to exploit, and intervention should not be completely off the table in cases where its value to the people most affected can be demonstrated. Ultimately, the crisis in Ukraine serves as a wake-up call: the West's hard- and soft-power capabilities must be developed and deployed proportionately while being underpinned by a comprehensive overarching strategy that defuses hostilities.

The Changing Geopolitical Context

Around the world, new powers are rising, with a complex geopolitical picture emerging. The US and China are the key superpowers, but they are far from the only actors. In terms of who poses the biggest challenges to the West, we focus below on recent military spending by Russia and China. These countries are on different trajectories, but are both examples of how new powers are outspending and outmanoeuvring the West.

Military Capability

Russia

When Vladimir Putin became the Russian president in 2000, the depleted armed forces that he inherited were a shadow of those at the disposal of his Soviet-era predecessors. The collapse of the Soviet Union and the economic depression that had plagued the Russian Federation in the decade that followed had stunted the development of its newly formed, independent military. Underfunded, over-reliant on poor-quality conscripts and armed with rusting hardware, the Russian forces entered the new millennium in a state of disarray. Heavy causalities sustained during the Chechen wars only added to the already dwindling morale among the Russian ranks, further highlighting to Putin the enormity of the rebuilding required to reassert military authority on the world stage.

Two decades on and the contrast could hardly be starker. During his annual press conference at the end of 2020, Putin proudly declared that "the situation has changed … Russia has one of the most efficient armies in the world". This was no exaggeration. Better drilled, technologically advanced and strategically capable, the Russian military machine had been modernised under Putin's command.

At the start of the second Chechen war, the Kremlin had approximately 1.4 million servicemen at its disposal, yet there were only 55,000 trained combat-ready troops among them. [4] The army was bloated with low-skilled conscripts, and the Kremlin therefore prioritised sweeping reforms to recruitment policies. Gradually, over the course of the past 20 years, Russia has professionalised its military by offering greater incentives for joining the armed forces, improving training programmes for new recruits and reducing service terms for conscripts. Though the Russian armed forces have slimmed down in overall size, they today contain a core group of more than 410,000 contract soldiers – a number which, as claimed by Russian Deputy Defence Minister Nikolai Pankov, "exceeds the number of conscripts by 1.8 times".

According to data from the Stockholm International Peace Research Institute (SIPRI), Russia's investment in its armed forces has averaged out at 4.1 per cent of its GDP over the past decade. [5] This dwarves the spending of any European democracy and, in relative terms, eclipses even the US – an indicator of Russia's policy priorities. Indeed, according to the Royal United Services Institute (RUSI), the British Army and its NATO counterparts do not have enough artillery and ammunition to maintain a credible defence position and would be "comprehensively outgunned" by Russia in serious conflict. This competitive edge is primarily due to Russia's improving economic fortunes at the turn of the millennium that has sustained a rate of spending reflected in a military that, as well as being better manned, is now seriously well-equipped. Today, Russia has the world's largest inventory of land forces including tanks, armoured vehicles, artillery and rocket projectors, more military aircraft than China and more naval vessels than the US. [6] Russia also continues to be the custodian of the world's largest stockpile of nuclear weapons, 5,977 in total – accounting for 47 per cent of the global nuclear arsenal – and, marginally, more than NATOs collective stockpile of 5,943. [7]

Russia's traditional logistical equipment and support services have been found wanting in Ukraine, and mechanical failures as a result of poor maintenance, support and planning have stalled the progress of Russian advances. Indeed, Russia has struggled to maintain consistent supply chains as it has advanced further and deeper into Ukraine which have forced units to pause and hold positions while they wait for the logistics to catch-up – leaving them vulnerable to Ukrainian resistance. While logistical issues have hampered Russia's invasion of Ukraine, and their armed forces have performed badly thus far, it is clear they have vastly improved their military capability.

Although the quality of Russian hardware fails in many cases to be as state-of-the-art as that owned by Russia's geopolitical competitors, it has improved drastically since the Chechen wars. As a result of heavy investment in research and development, the T-72B3 tanks currently rolling through Ukraine have guided missiles with twice the range of most tanks while the new Russian manufactured T-14 Armata tank, scheduled to go into mass production this year, has been claimed to rival the best in the world. [8] After launching the first prototypes in 2012, in 2018 Russia claimed it had trumped the US in the race to build the world's first intercontinental hypersonic missiles, which can fly at speeds to evade even the most advanced US radars and anti-missile defence systems. "No one listened to us," claimed Putin at their unveiling, which included a video simulation of a missile bound for the US, before going on to demand, "Listen to us now". [9]

After beginning testing in 2014, [10] China too was able to launch a successful hypersonic missile test in 2021, which prompted General David D Thompson of the US Space Force to admit that, "we're not as advanced as the Chinese or the Russians in terms of hypersonic programs" and the US has "catching up to do very quickly". [11] Compared to the US, Russia and China have an easier time navigating the scrutiny of lawmakers and the general public, which allows them to accelerate the development of their weapons

programmes. The US is, however, now investing billions in playing the game of catch-up, with an aggressive effort being made to ensure hypersonic operational capability by September 2022.

The pursuit of technological advancements has also upgraded Russia's non-conventional military capabilities, including cyber-warfare tactics used extensively over recent years as a powerful tool for destabilising foreign infrastructure and undermining democratic processes.

Russia's military might and influence extends beyond surface-level capabilities. For years, the Kremlin has leveraged Russian pseudo-private paramilitaries, principally the Wagner Group, to advance its foreign-policy agendas overseas. These groups may brand themselves as guns for hire, but their management and operations are deeply entwined with the Russian military and intelligence community – and are at the beck and call of Putin. As well as being cheaper and more flexible than conventional military forces, the deployment of these private groups gives the Kremlin plausible deniability while furthering its national interests, without direct involvement. The Wagner Group worked alongside Russian forces during the annexation of Crimea in 2014, and has been deployed in Syria, Libya and Mali to carry out frontline warfare, hostile reconnaissance, sabotage and false-flag operations.

Servicemen enlisted with the Wagner Group, who are typically retired Russian military personnel, are reported to be paid between 80,000 to 200,000 Russian roubles a month. The capability the Kremlin has of being able to deploy a force like this to fight on the ground is something the West has no direct answer to. Despite the enormous effort made in upgrading the military, there is no hiding from the fact that Russian forces have not performed well in Ukraine – much to the frustration of Putin. This reality can be attributed to several factors, principally that the invasion strategy was flawed and built on a number of erroneous assumptions, including the idea that Russian troops would be met with token resistance – an assumption that couldn't have been further from the reality they've encountered. In a conflict such as this, traditional military doctrine would make the case for heavy use of combined arms – a joined-up, systematic deployment of different military elements, infantry, tanks and aircraft. However, at least in the early days of the war, this was not the case. Instead, isolated groupings of paratroopers and tanks were sent to the front lines with insufficient logistical support to back them up, and they confronted a better armed and more resolute resistance than had been anticipated.

China

China's military is expanding – and modernising – at pace. The country now ranks second in the world for military expenditure, outstripped only by the US, with increases of its military budget having outpaced its overall economic growth for at least a decade. President Xi's military ambitions are baked into his core vision for China's future, the "Two Centenary Goals", which calls for "complete military modernisation" by 2035 and a "world-class military" by 2049.

It's important not to fall into lazy comparisons with Russia, however. Unlike Putin and his circle, Chinese diplomatic and military thinking is characterised by a fierce aversion to overt interventionism (Taiwan is potentially an exception because, in Beijing's eyes, it is a domestic matter). Rather, Beijing's military doctrine stresses information dominance and "winning without fighting" to the extent that the rapidly expanding People's Liberation Army (PLA) has never been tested on the modern battlefield.

Beijing has yet to find itself cornered: for now, the global status quo mostly continues to benefit China in ways it doesn't Russia. In other words, this is a question of balance for Western countries: they should avoid conflating China's military ambitions with Russia's, but they should also avoid blind faith in Beijing's "peaceful partner" pitch, too.

This will mean staying ahead of the curve as China's military evolves. China has been making remarkable progress towards its two centenary goals, investing in hypersonic-missile capacity, launching a burgeoning aircraft-carrier programme and building the world's largest (if not yet most powerful) navy. The US Navy predicts the number of Chinese navy ships will increase by nearly 40 per cent by 2040, cementing China's position as the dominant regional power.

Significant – if disputed – progress is also being made on China's nuclear capabilities. In late 2021, the US Department of Defence warned that China was to quadruple its stockpile of nuclear warheads by 2030. Chinese authorities, keen to stick to their long-standing line of "nuclear minimalism", have insisted that new missile silos are actually wind farms. The truth is somewhere in between: while there is broad consensus that China is unlikely to deviate from its no first-use policy, the SIPRI have found credible evidence that China has been increasing warheads in recent years. Whatever the exact figures, China is settling in for what it sees as a prolonged – if not permanent – period of heightened hostility with the US.

Equally pressing is China's pursuit of newer, cyber-centric forms of warfare. China has already launched large-scale cyber-operations abroad, conducted by military groups and state-backed civilian actors that profit from increasingly blurred lines between the civil and military spheres. And it's not just behind the scenes where these lines are blurred: under Xi, authorities have increasingly pushed the idea of "military-civil fusion", easing the administrative burdens on private tech and defence companies in order to encourage greater military innovation and collaboration.

Military theorists also speak glowingly of "intelligisation", a vague term that focuses on the potential transformative role of artificial intelligence in Chinese military strategy. Here, the intention is to leapfrog Western militaries, developing advanced algorithms and highly centralised decision-making structures that can help commanders direct military action automatically.

China is not set to fully outstrip US military capabilities soon although the gap is closing. Many of the most ambitious "intelligisation" proposals remain technologically far-fetched, and even the most advanced tech will struggle to overcome the rivalry and parochialism that continues to hinder the PLA's

ability to carry out effective joint operations. But the big question is, how much does out-and-out competition with the US actually matter to Beijing?

The 2049 centenary goal aims for a "world class" – not a "world leading" – military. Unlike Moscow, Beijing has little desire to be wilfully antagonistic when it can avoid it. Instead, Beijing sees its growing military strength as a security guarantee, part of a broader platform of military, diplomatic and economic levers that can be pulled primarily to ensure the security of its regional interests and, most importantly, serve as a display of force on its top priority – Taiwan.

Cyber and Hybrid Threats

Over the past 20 years, the nature of geopolitical interactions had been characterised by a persistent state of "unpeace". In this zone, actions falling just short of war are deployed to undermine the stability of states: they sufficiently disrupt the equilibrium but fall below the threshold that would make military retaliation politically feasible or rational. It is estimated that malicious cyber-activity costs the world $945 billion annually. [12]

Cyberspace lies at the heart of these activities, both as a domain of conflict and an enabler of warfare. While the Ukraine crisis has highlighted the limitations of cyber-operations during active conflict, the threat of state or state-sponsored and non-state cyber-operations as an accompanying tool is real.

States able to coordinate their capabilities, such as Russia and China, are quickly working to gain the upper hand dominating this grey zone. The US maintains its position as the leading global cyber-power – according to the Belfer National Cyber Power Index [13] and a recent cyber-capabilities assessment by the International Institute for Strategic Studies (IISS) [14] – with its offensive capability stronger than any other country. [15] But according to the Belfer index, the UK ranks between China (second) and Russia (fourth), which are rapidly closing the gap, and European countries are falling behind.

The UK has reinforced its vision, as per the Integrated Review 2021, of being a responsible cyber-power, [16] with the National Cyber Strategy 2022 allocating £2.6 billion funding for cyber-policy and an additional £114 million for the National Cyber Force. Meanwhile, the White House has requested $9.8 billion from Congress to support civilian cyber-security. [17] Similarly, the Digital Europe Programme (2021-2027) has committed €1.9 billion to cyber-security capacity and the deployment of related infrastructure and tools across the EU for public administrations, businesses and individuals. [18] To ensure strong defensive capability, part of this spending must focus on developing strong standards for threat-information sharing between allies and intelligence partners. This should align with active participation to strengthen the cyber-norms regime, including the current negotiations on the new UN Cybercrime Convention and the third version of the Talinn manual, to seek greater clarity for the range of responses

available in event of malicious cyber-operations that violate international law. While collaborative cyber-resilience will be key to defending forward and deterring by denial against the expanding and creative threats we outline below, greater clarity on the possibilities for coordinated response will be critical to ensuring strategic dominance in this sphere.

Russia

Russia has a sophisticated network of units under its security and intelligence agencies, which can conduct disinformation, propaganda and espionage activities globally. The federation also relies upon criminal and civilian hackers to engage in action that extends its reach, affording it plausible deniability when needed. Russia's cyber-strategy has largely set out to sow discord and confusion among its opponents, and undermine Western democracies.

Russia's early operations relied upon distributed denial-of-service (DDoS) attacks, which bring down websites or services to make them unavailable. They were first experienced at significant scale in the 2007 cyber-attack on Estonian banks, media and government bodies, in response to the country's removal of a Soviet-era statue. Then, while Russia denied responsibility for the cyber-attacks on Georgia during its 2008 war with the country, 54 targets were hit in parallel with Russia's military actions, resulting in the National Bank of Georgia having to suspend all electronic trading for 12 days.

Over the past 20 years, Russia has invested significantly in its cyber-capabilities across several intelligence agencies, from the Main Intelligence Directorate of the Russian army (GRU), Foreign Intelligence Service (SVR), Federal Security Service (FSB) and Federal Protective Service (FSO) to the privately funded Internet Research Agency (IRA). The IRA, Russia's notorious troll farm or factory, funded by oligarch Yevgeny Prigozhin, focuses on global disinformation and the impersonation of domestic activists to undermine political processes, including during the 2016 US presidential election when its activities took place alongside hacking by SVR cyber-units. [19]

Acting both in tandem and competition, these units have been operating with increased aggression and are responsible extremely harmful cyber-attacks around the world. Ukraine has often been a testing ground, with regular attacks on its critical infrastructure. [20] The 2017 NotPetya malware attack, [21] linked to a GRU unit, started as an attack in the Ukraine but led to losses of $10 billion globally, with Maersk shipping sustaining between $250 and $300 million of economic damage.

The 2020 attack on Texas-based SolarWinds, designed to exploit supply-chain vulnerabilities and infiltrate US government and private-sector networks, was attributed to Russian hacker group APT29 and demonstrated a stealth-based strategy that, according to Silverado Policy Accelerator's Chairman Dmitri Alperovitch, signifies increasing Russian technical sophistication. [22] According to Microsoft's Digital Defence Report 2021, 58 per cent of all global cyber-attacks on nation states that could be

identified originated in Russia. [23] While Russia's new shift to covert cyber-operations may be driven by increased technical capability rather than a deliberate strategic shift, it is now focusing on advanced intrusion tactics, according to the cyber-security expert Professor Josephine Wolff. These include account harvesting, supply-chain interference and infiltrating critical service providers – and are in place of attacks on infrastructure that could backfire on the SVR. [24]

Russia also continues to expand its reach by supporting criminal organisations within its borders to launch destructive cyber-crimes on overseas critical infrastructure, which have included the Darkside gang attacking Colonial Pipelines in May 2021, resulting in 45 per cent of the fuel supply to the US's East Coast being compromised, and in the same year, REvil's attack on the JBS meat-processing company based in Brazil. Collectively, these criminal organisations have extracted over $1 billion in ransoms by targeting thousands of companies. [25]

Russia's investment in developing this capability means the threat of retaliatory cyber-operations that inflict significant economic damage on Western allies is highly credible, especially during periods of antagonism that the West is experiencing today.

China

With the world's largest number of internet users, China's interest in the cyber-domain was originally rooted in a strategy to preserve cyber-sovereignty, and prevent foreign information and influence. With cyberspace viewed as one part of its broader information space, China's strategic goal is to control information rather than to control cyberspace itself.

While the IISS's 2021 report places China approximately ten years behind the US in strategic capability, [26] as coming in second on the Belfer Center's Cyber Power Rankings in its intent to employ its growing capability, [27] experts now view it as the most formidable adversary to the US in cyberspace. [28] This is reflected in the expansion of its cyber-enabled espionage operations, including intellectual-property theft, personal-data extraction and access to strategic systems, [29] and its stated goal of maturing into a cyber-superpower by 2035, as per the 14th Five-Year Plan. [30]

Unlike Russia, China's large-scale cyber-espionage activities have been used to further its ambition to gain supremacy as a military and economic superpower, rather than to sow discord and instability. Between 2010 and 2015, China targeted US and European aerospace companies to steal intellectual property that was then funnelled back to its own manufacturers. It has built on its systematic programme of espionage and theft, such as the 2015 Equifax hack of nearly 150 million Americans' personal data, to target strategically important industries and institutions including defence and semiconductor firms, medical institutions and universities. [31] It expands its potential reach through local bug-bounty competitions, such as the Tianfu Cup. These competitions, which invite hackers to find new flaws in

software code in return for cash, have provided China with early access to valuable previously unknown vulnerabilities, such as the compromising of the Apple iPhones of Uyghur minority targets, with a vulnerability revealed by the competition in 2018. [32] This seems to be underpinning the republic's new wave of offensive cyber-capabilities that have ranged from the exploitation of Microsoft Exchange Server vulnerabilities by the Chinese hacker group Hafnium, affecting up to 250,000 organisations in March 2021, [33] to the China-backed APT41 breaching at least six US government networks between May 2021 and February 2022. [34]

These increasingly provocative actions, alongside a programme to acquire a cutting-edge cyber-talent pool, signal the strength of China's potential cyber-arsenal and its intention to assert its offensive capability more firmly.

How Has the West Fallen Behind?

We should be cautious about speaking of a homogenous West. Indeed, one of the ways in which the West has fallen asleep is through the lack of an overarching defence strategy as well as coordination among allies in our hemisphere and the Indo-Pacific region. For these purposes, however, we focus on the West in the specific sense of the US, EU and UK, and alliances such as NATO, to show how Western powers are falling behind – in comparison to countries like Russia and China.

It is not simply a question of capabilities. The West also needs to understand what its goals are, and the lengths it is willing to go to achieve them. Specifically, the lack of political will in Western democracies to defend our values abroad has opened a power vacuum in areas of the world that Russia, and to some extent China, have sought to fill.

Without being able to show that it is willing to follow through in defence of the values it preaches, the West risks giving up more ground to nations that will. NATO and its allies must be prepared to stand up for values that are fundamental to global security. To this end, Phil Wilson, a former member of the House of Commons Defence Committee, stated, "If we are to maintain our unity of purpose, we must understand what that purpose is: it is human rights, democracy, the rule of law and our much-cherished way of life so easily taken for granted. If the West does not stand by those principles, no one else will."

What Role for the US?

American decline, a concept debated by friends and enemies of he US, encapsulates the idea that the US is diminishing in power geopolitically and militarily due to declining military advantages, economical capabilities and economic relationships. The prospect of American decline is exacerbated by a growing sense of Washington's diminished willingness to employ its power and resources abroad in support of its global presence.

The US military has gone through multiple transitions over the past 20 years. Though expenditure as a percentage of GDP has been well above other NATO allies, the focus and investment of the US Department of Defense has not always aligned with the strategic needs of the future.

This was evident as the US began to pivot away from a focus on combatting terrorism towards counterinsurgency in Iraq and Afghanistan, and today back towards the realm of great-power confrontation. With its attention on China, which many see as the primary 21st-century competitor to the US, the country has ended up creating space for Russia's growing military threat.

The US still maintains the most powerful military in the world, with an active fighting force of 1.4 million people, which is only marginally larger than Russia's 1 million active troops. However, as of January 2022, Russia had an estimated military personnel of 3.6 million in total, second only to China's 4 million military personnel while, in relation to land power, Russia had 2,249 more infantry fighting vehicles than the US. But while the US has an estimated 2.2 million military personnel, its competitive advantage in strategic areas and geopolitical theatres has been waning as the conflicts in the Middle East have raged on. From cyber-warfare to projecting force in the Indo-Pacific, from artificial intelligence to hypersonic technologies, the US has lost ground to regional and global adversaries. While remaining superior militarily when it comes to global projection, logistics and precision-strike capabilities, adapting to new and unconventional methods of war must also be a future priority.

Following its rapid rise in military strength and ability to project force into new theatres, China is increasingly beginning to bristle when it sees US influence encroaching on its spheres of influence, particularly in the South China Sea. Russia's invasion of Ukraine pushes the limits of Western, and perhaps most importantly US, resolve in the face of a challenge to the current world order.

The US Department of Defense acknowledged in its Interim National Security Strategic Guidance last year that investments must be refocused to address the coming of great-power conflicts of the 21st century. [35] However, simply increasing the budget more is not the answer. While the official national strategy is still being produced, lessons from the past six months should be fully understood and applied.

The US must coordinate with its allies, those in Europe as well as in Asia and the Indo-Pacific, in ways that maximise each country's strategic advantages while supporting the shortfalls in each other's defences. The US will inevitably be the main driver of both coordination as well as support for other nations, but strong alliances built on integration and strategic cooperation can better prepare the West for the challenges to come.

President Biden has worked to rebuild Western alliances in light of the Ukraine crisis, but more is needed, as other NATO members will need to rise to the occasion and take more of the initiative.

Defence Spending by NATO Members Has Been Too Low for Too Long

While NATO remains the most powerful military alliance in the world, years of complacency and misalignment on strategic goals have weakened its dominance. Before the end of the Cold War, Western European nations spent on average 2.4 per cent of their GDP on their military. However, this had declined to an average of just 1.6 per cent by 2020. Currently, only 10 member countries (out of 30) meet the target to spend at least 2 per cent of their GDP on defence.

Figure 2 – Rates of GDP spending on defence among major NATO members

Country	2015	2016	2017	2018	2019	2020
France	1.9%	1.9%	1.9%	1.8%	1.8%	2.1%
Germany	1.1%	1.1%	1.2%	1.2%	1.3%	1.4%
Italy	1.2%	1.3%	1.4%	1.4%	1.3%	1.6%
UK	2.0%	2.0%	1.9%	1.9%	2.0%	2.2%
Poland	2.1%	1.9%	1.9%	2.0%	2.0%	2.2%
USA	3.5%	3.4%	3.3%	3.3%	3.4%	3.7%
Canada	1.2%	1.2%	1.4%	1.3%	1.3%	1.4%

Source: https://www.sipri.org/databases/milex

The invasion of Ukraine has prompted drastic changes in European defence spending. For example, Germany has pledged to re-arm itself by spending over 2 per cent a year on defence as well as to ship arms to Ukraine. But other NATO members should follow suit and spend that money smartly.

Investing money in ways that best address the challenges the alliance is likely to face this century is essential. To this end, EU governments should explore ways in which member states can better integrate their defence infrastructures, including through increased investment in cyber-warfare and countering disinformation, both in members states and more widely. Ensuring that the EU bloc is equipped to defuse hostilities before military escalations, and more effectively dissuade reactionary forces and would-be threats, is a development that must be rooted in an understanding of the strategic advantages and domestic context of each member state – in relation to the rest of the world.

EU Defence Policy

Speaking at a defence conference in December 2021, High Representative of the European Union for Foreign Affairs and Security Policy Josep Borrell Fontelles, highlighted some of the issues the EU is having: "Comparing the European Union and its member states with other global actors, we see that we lag far behind in terms of investing in defence innovation. And this gap is widening." [36]

Following the global financial crash of 2008, defence spending declined in many European countries. According to the Center for Strategic and International Studies (CSIS), defence spending plummeted by 3 per cent in 2009 and continued to steadily decline until 2013 across Europe. [37]

The CSIS report found the trend was the most pronounced among smaller European nations, for example, in Lithuania, where defence spending was cut by more than 36 per cent in 2010. Although defence spending did begin to rise post-2013, it took until 2018 for European defence expenditure to recover to its (already low) pre-2008 level. [38]

These cuts are reflected in what a Center for American Progress report describes as "a readiness crisis", [39] referencing a 2017 Munich Security Conference report that stated: "A post-Cold-War focus on expeditionary operations and the constraints of austerity came at the expense of equipment availability across many weapon systems. For example, in some states, up to half of helicopters or infantry fighting vehicles are not deployable." [40]

Over the past two decades, European armies have collectively lost 35 per cent of their capabilities. [41]

For the EU, the story since 2016 has been one of focusing on "strategic autonomy". Stung by both Trump and Brexit, expanding Chinese economic might and the AUKUS (Australia, UK and US) defence alliance, European nations have turned inwards to assess how to strengthen their own capabilities. Within the EU, the focus has been on the €8 billion European Defence Fund, of which €2.7 billion is designated to collaborative research and development and €5.3 billion to collaborative capability development. [42] These priorities for 2021 included development of the French, German and Spanish sixth-generation fighter aircraft, and research into modular, unmanned and beyond-line-of-sight ground-combat capability.

While this additional EU-level investment is welcome, it has three fundamental problems. First, the scale of funding provided is not sufficient to close the spending gap described above. Second, it does not include key partners including the UK. Last, member-state governments mistake additional defence spending at the EU level and the concept of sovereign autonomy on defence industrial capabilities for the ability to provide an effective security umbrella against external threats.

The Wake-Up Call for a New Strategy

The West has been neglecting the issue of defence while other powers, such as Russia and China, are advancing. The Ukraine crisis, alongside the Afghanistan withdrawal, should serve as a wake-up call for Europe, the US, the UK and our allies.

What is required is a reconsidered strategy that combines reconsidered spending commitments, the right capabilities and far-reaching coordination.

But Not a Strategy That Leaves Us on the Back Foot

The Russian invasion of Ukraine has galvanised Western democracies, reawakened old alliances and strengthened the commitment to collective policymaking on issues of defence and security through institutions such as NATO. Putin did not anticipate such a defiant demonstration of unity from the US and Europe. However, this image will only last as long as the West works collectively on global security and in the long-term defence of liberal democratic values. Lasting European security cannot be permanently based on US guarantees alone.

At present there are several discrepancies between the priorities outlined in the national-security and defence strategies of Western powers, including the US, UK, EU, France and Germany, as well as NATO's strategic vision. Beyond increases in national defence budgets, practical steps to refresh and strengthen the strategic frameworks that underpin European security should include:

- Signing a comprehensive UK–EU defence and security agreement
- Inviting all NATO countries that are not EU members to participate as equal partners in the European Defence Fund
- Building on the E3 (UK, France and Germany) format (plus the US and NATO) to identify and pursue strategic military and political priorities for European security

These steps will go some way to addressing the biggest weakness in Western strategy: the inability to think about foreign, defence and security policy from different geographical perspectives, or in the context of shifting global power dynamics. Our defence and security needs to evolve to account for the return of great-power rivalry or, at the very least, a far more fragmented global order.

Alongside increased defence spending, the West must also improve the strategic framework guiding our spending decisions, enabling power and force projection, and providing the basis for global coordination and coalition building.

The national-security and defence strategies of major Western powers are generally predicated on a values-based approach to foreign policy. The UK's recent Integrated Review outlines a progressive vision of a global Britain committed to standing up for democratic values and freedoms. In recent years, to deliver on this mandate, the West has prioritised soft-power foreign-policy levers and, where it does engage militarily, over-the-horizon capabilities. However, in the face of direct aggression that undermines the values we seek to promote in the long-term, the West must be prepared to employ appropriate measures in the short-term.

But we also need to prepare for other potential flashpoints requiring a different – albeit similarly coordinated – approach. Parallels between Ukraine and Taiwan are often overplayed, but Taiwan is the one area that could feasibly bring us into conflict with an otherwise "peaceful" China in the medium-term. The conflict in Ukraine is likely sending a message to Beijing about the West's ability to act in concert, but it's also giving it an insight into our toolkit. Western leaders need to have a credible, coordinated plan in place to prevent tensions escalating with the world's second-largest military power.

Smarter Spending

Countries must ensure that a reasonable increase in defence spending remains a priority, with NATO members each making a proportionate contribution. This must be linked closely to putting in place the right capabilities because how we spend the NATO budget is as important as the money itself.

Defence-spending priorities should be guided by a wider, strategic agreement on sustaining European security rather than siloed, inward-looking concepts such as Global Britain or Europe's strategic autonomy. Coordination on defence spending could ensure equipment and support services that are interoperable while also maintaining individual and collective operational advantage, and freedom of action.

European countries have already made considerable progress on this front since 2014, with 2021 being the seventh consecutive year of defence-spending growth. Not only has there been cumulative extra contribution of $190 billion since 2014, but NATO countries in Europe have also invested in major equipment, taking steps towards fairer burden-sharing. [43]

Russia's invasion of Ukraine has prompted European leaders to reconsider EU defence policy even further. German Chancellor Olaf Scholz has announced that a fund of €100 billion (£85 billion) will be set up immediately to boost the strength of the country's armed forces and he has pledged to spend 2 per cent of Germany's GDP on defence annually. [44]

Similarly, in a press conference on 6 March, Danish Prime Minister Mette Frederiksen announced that Denmark will increase its defence spending over the next few years until it reaches 2 per cent of GDP by 2033, in line with the goal set out by NATO. [45]

These changes are steps in the right direction. But they must come alongside a sensible approach to shared defence, and one significant element of effective spending is greater coordination between the EU and NATO. Europe's investment in existing NATO structures is far more practical than the bloc trying to replicate them at an EU level. Going forward, the Russian invasion should serve as a wake-up call that increased spending needs to be matched by an increased focus on outward-looking, coordinated strategy.

Developing Comprehensive Capabilities

Development for the West needs to focus more on a comprehensive set of capabilities for integrated use across the full spectrum of conflict, including on land, at sea and in the air as well as in space and cyberspace. Additionally, it is imperative to have conventional and nuclear forces available.

Efforts to improve NATO's capabilities have been at the forefront of recent discussions responding to the invasion of Ukraine. For example, the capability to reinforce NATO's eastern flank is being improved by the coordination of strategic and operational movements, developed legislation and procedures, and better host-nation support and exercises. However, inadequate infrastructure and a dearth of readily available transport options continue to impose severe limits to this effort.

NATO must continue with investment in and development of modern battle frontiers, particularly cyber-warfare, and recognise how areas such as transport could be strengthened in order to respond to future conflicts. NATO should increase cyber-exercises including by expanding its Cooperative Cyber Defence Centre of Excellence and providing support to non-NATO allies to adequately develop their defences.

In developing these new capabilities, quantity should not be overlooked. A strong physical military presence is still considered a key indicator of power. Investment in artillery, ships, planes and troops, which are all conventional defence priorities that have been overlooked in recent years, should be renewed and positioned as part of any modern capability agenda.

Ensuring Ongoing Coordination

None of this will be effective without proper coordination among and within EU and NATO countries. Recognising this, Italian Prime Minister Mario Draghi told the Italian Senate on 1 March: "Today's threat from Russia is an incentive to invest more in defence than we have ever done before. We can choose whether to do this at a national or European level. My hope is that all countries will increasingly choose to adopt a common approach." [46]

The conflict has exposed the lack of preparedness for supranational organisations to meet the challenges of military threats from rogue powers. In order to ensure that the post-war rules-based order is upheld, there must be greater coordination of defence policy going forward. This should include hastening the reform of the EU's Common Security and Defence Policy, and expanding EU membership to include countries with a shared sense of internationalism and respect for the rule of law.

Cohesion of NATO demands solidarity and burden-sharing, and there is a need for pre-planned options that allow for quick and effective actions to be taken by coalitions.

Within NATO, efforts need to be made to improve the speed of decision-making by promoting intelligence-sharing, delegating authority to the Supreme Allied Commander Europe (SACEUR) and agreeing on the indicators for an armed attack. For example, there is currently uncertainty concerning the chain of command, with no given headquarters responsible for leading land or joint operations in Northern Europe.

Conclusion

As this paper makes clear, the West has lacked a coherent and coordinated defence strategy in recent years. This absence has seen us less able to project our values around the world – and to defend them. The result has been space opening up for those who don't share our values. Bluntly, democracies have been on the back foot, with more authoritarian regimes able to operate in more agile ways and commit to more spending. The Ukraine crisis must prompt a change in this trajectory.

Baron West of Spithead, a retired Royal Navy admiral, spoke with us about this paper and commented: "The Ukraine crisis should serve as a wake-up call to politicians and opinion formers. In response the UK and NATO need to invest now in the necessary capabilities and strategies to meet the threats we face."

Such a wake-up call can only be heeded through coordination and international action. The West, through our democratic values, has important assets that we should not forget. Indeed, these are something to fight for. We have collective strength in our ability to be creative, to collaborate and influence countries around the world through the right combination of hard and soft power.

This paper sets out the path to achieve this.

Recommendations

Keep up the momentum: Russia's invasion of Ukraine has galvanised the West. Measures such as signing a comprehensive UK–EU defence agreement and inviting non-EU NATO members to participate as equal partners in the European Defence Fund will help ensure ongoing strategic alignment.

Prepare for future flashpoints: Responding to China will require a different set of tools than to Russia. Countries should have a credible and coordinated plan in place to prevent tensions over Taiwan escalating to the point of military conflict.

Spend smarter: Any increases to defence funding must keep coordination and shared defence in mind, ensuring that new equipment and support services are interoperable.

Develop comprehensive capabilities: Western countries should continue to strengthen conventional capacity across land, air and sea while developing new approaches to modern battle frontiers, particularly cyber-warfare.

Improve coordination: Supranational organisations, in particular NATO, need to speed up decision-making, promote intelligence-sharing and clarify chains of command.

Keep values at the heart of military strategy: We must be ready to promote and defend the values we believe in. NATO should issue a collective mission statement that sets out how our military strategy can work in service of a broader mission to promote democracy and equality worldwide.

Footnotes

1. ^ https://www.institutmontaigne.org/en/blog/5-years-macron-zooming-french-defense
2. ^ https://sipri.org/databases/milex
3. ^ https://www.aei.org/research-products/report/the-defenders-dilemma-defining-identifying-and-deterring-gray-zone-aggression/
4. ^ https://www.wsj.com/articles/russia-confronts-ukraine-with-upgraded-military-rebuilt-after-soviet-collapse-11643733217
5. ^ https://www.sipri.org/databases/milex
6. ^ https://www.globalfirepower.com/
7. ^ https://fas.org/issues/nuclear-weapons/status-world-nuclear-forces/
8. ^ https://nationalinterest.org/blog/buzz/russias-new-armata-t-14-tank-how-worried-should-army-be-190041
9. ^ https://www.nytimes.com/2022/01/27/world/europe/russia-military-putin-ukraine.html
10. ^ https://www.nytimes.com/2021/10/27/us/politics/china-hypersonic-missile.html
11. ^ https://www.politico.com/news/2021/11/20/hypersonic-technology-us-behind-china-russia-523130
12. ^ https://www.forbes.com/sites/jonathanponciano/2022/03/07/extremely-destructive-russian-cyberattacks-could-cost-us-billions-of-dollars-in-economic-damage-goldman-warns/?sh=7906f43b2dc0
13. ^ https://www.belfercenter.org/publication/national-cyber-power-index-2020
14. ^ https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power
15. ^ https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power
16. ^ https://www.gov.uk/government/publications/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy
17. ^ https://www.fedscoop.com/white-house-allocates-9-8b-to-cybersecurity-in-2022-budget-request/
18. ^ https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies#https://digital-strategy.ec.europa.eu/en/activities/digital-programme

19. ^ https://crsreports.congress.gov/product/pdf/IF/IF11718
20. ^ https://sgp.fas.org/crs/homesec/R46974.pdf
21. ^ https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
22. ^ https://www.csis.org/events/evolution-russian-cyber-tactics-and-operations
23. ^ https://blogs.microsoft.com/on-the-issues/2021/10/07/digital-defense-report-2021/
24. ^ https://www.fpri.org/article/2021/07/understanding-russias-cyber-strategy/
25. ^ https://www.foreignaffairs.com/articles/united-states/2021-12-14/case-cyber-realism
26. ^ https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power
27. ^ https://www.belfercenter.org/publication/national-cyber-power-index-2020
28. ^ https://www.foreignaffairs.com/articles/united-states/2021-12-14/case-cyber-realism
29. ^ https://carnegieendowment.org/2021/07/06/west-should-not-be-complacent-about-china-s-cyber-capabilities-pub-84884
30. ^ https://www.osti.gov/servlets/purl/1830481
31. ^ https://www.foreignaffairs.com/articles/united-states/2021-12-14/case-cyber-realism
32. ^ https://warontherocks.com/2021/10/china-flaunts-its-offensive-cyber-power/
33. ^ https://www.csoonline.com/article/3616699/the-microsoft-exchange-server-hack-a-timeline.html
34. ^ https://thehackernews.com/2022/03/chinese-apt41-hackers-broke-into-at.html?_m=3n%2e009a%2e2692%2ebu0ao444z6%2e1psr
35. ^ https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf
36. ^ https://eeas.europa.eu/headquarters/headquarters-homepage/108482/european-defence-agency-speech-high-representativevice-president-josep-borrell-annual_en
37. ^ https://www.csis.org/analysis/toward-new-lost-decade-covid-19-and-defense-spending-europe
38. ^ https://www.csis.org/analysis/toward-new-lost-decade-covid-19-and-defense-spending-europe
39. ^ https://www.americanprogress.org/article/case-eu-defense/
40. ^ https://issuu.com/munichsecurityconference/docs/europeandefense_more_european_more_

41. ^ https://www.csis.org/analysis/toward-new-lost-decade-covid-19-and-defense-spending-europe
42. ^ The European Defence Fund (EDF) (europa.eu)
43. ^ https://www.nato.int/cps/en/natohq/topics_133127.htm
44. ^ https://www.nytimes.com/2022/02/27/world/europe/germany-military-budget-russia-ukraine.html
45. ^ https://www.politico.eu/article/denmark-to-increase-defense-budget-and-phase-out-on-russian-natural-gas/
46. ^ https://cepa.org/italy-must-raise-defense-spending-to-historic-levels-draghi-says/

FOLLOW US
facebook.com/instituteglobal
twitter.com/instituteGC
instagram.com/institutegc

GENERAL ENQUIRIES
info@institute.global

FIND OUT MORE
INSTITUTE.GLOBAL