The War in Ukraine: Reality Check for Emerging Technologies and the Future of Warfare

Geneva Paper 34/24

Jean-Marc Rickli and Federico Mantellassi

April 2024

GCSP
Geneva Centre for
Security Policy

The Geneva Centre for Security Policy

The Geneva Centre for Security Policy (GCSP) is an international foundation that aims to advance global cooperation, security and peace. The foundation is supported by the Swiss government and governed by 54 member states. The GCSP provides a unique 360° approach to learn about and solve global challenges. The foundation's mission is to educate leaders, facilitate dialogue, advise through in-house research, inspire new ideas and connect experts to develop sustainable solutions to build a more peaceful future.

The Geneva Papers and l'Esprit de Genève

With its vocation for peace, Geneva is the city where states, international organisations, NGOs and the academic community work together to create the essential conditions for debate and action. The Geneva Papers intend to serve this goal by promoting a platform for constructive and substantive analysis, reflection and dialogue.

Geneva Papers Research Series

The Geneva Papers Research Series is a set of publications offered by the GCSP.

The Geneva Papers Research Series seeks to analyse international security issues through an approach that combines policy analysis and academic rigour. It encourages reflection on new and traditional security issues, such as the globalisation of security, new threats to international security, conflict trends and conflict management, transatlantic and European security, the role of international institutions in security governance and human security. The Research Series offers innovative analyses, case studies, policy prescriptions and critiques, to encourage global discussion.

This series is edited by Dr. Jean-Marc Rickli, Head of Global and Emerging Risks.

All Geneva Papers are available online at:
www.gcsp.ch/publications

ISBN: 978-2-88947-122-5

The views, information and opinions expressed in this publication are the authors' own and do not necessarily reflect those of the GCSP or the members of its Foundation Council. The GCSP is not responsible for the accuracy of the information.

Cover photo: Getmilitaryphotos, Envato Elements

About the authors

Dr Jean-Marc Rickli is the Head of Global and Emerging Risks and the Founder and Director of the Polymath Initiative at the GCSP. He is also the co-chair of the Partnership for Peace Consortium (PfPC) Emerging Security Challenges Working Group and a senior advisor for the Artificial Intelligence Initiative at the Future Society. He is the co-curator of the International Security Map of the Strategic Intelligence Platform of the World Economic Forum. He is also a member of the Geneva University Committee for Ethical Research and of the advisory board of Tech4Trust, the first Swiss startup acceleration program in the field of digital trust and cybersecurity. Prior to these appointments, Dr Rickli was an assistant professor at the Department of Defence Studies of King's College London and at the Institute for International and Civil Security at Khalifa University in Abu Dhabi. In 2020, he was nominated as one of the 100 most influential French-speaking Swiss by the Swiss newspaper *Le Temps*. Dr Rickli received his PhD in International Relations from Oxford University. His latest book published by Georgetown University is entitled *Surrogate Warfare: The Transformation of War in the Twenty-first Century*.

Mr Federico Mantellassi is a Research and Project Officer at the Geneva Centre for Security Policy where he has worked since 2018. Federico's research and writing focuses on how emerging technologies impact international security and warfare, as well as on the societal implications of their development and use. Federico is also the project coordinator of the GCSP's Polymath Initiative; an effort to create a community of scientists able bridge the gap between the scientific and technological community and the world of policy making. Previously, he assisted in the organisation of executive education activities at the GCSP and was the project coordinator of the annual Geneva Cyber 9/12 Strategy Challenge. He holds a Master's Degree in Intelligence and International Security from King's College London, and a Bachelor's Degree in International Studies from the University of Leiden. Federico speaks English, French and Italian.

Acknowledgements

The authors would like to extend their thanks to Mr Miras Makitov and Mr Valentin Julliard for their valuable background research which contributed to the realisation of this paper, and to Mr Eden Cole for his comments.

Contents

I. Introduction

Russia's full-scale invasion of Ukraine in February 2022 marked the beginning of one of the most intense and brutal state-on-state conflicts opposing two modern militaries in recent memory. Despite Russia's qualitative and quantitative advantages, Ukraine's armed forces have so far put up strong resistance, foiling Russian plans of a quick victory and turning the conflict into a bloody war of attrition. Due to its scale and the nature of its belligerents, the conflict can provide us with a glimpse into what the future of warfare might look like and help us recentre the burgeoning conversation about the future of warfare in the current reality, especially as it relates to the presence and impact of emerging technologies. The war therefore offers us a way to understand how digital and off-the-shelf technologies such as artificial intelligence (AI) impact conflicts of this scale and how relevant they are to current modern warfare. The war can also help us see how new actors become involved in warfare, what new means of influencing nation states are becoming available, and which new tools armed forces can use to affect battlefield outcomes. Importantly, it can help us gauge their importance relative to more traditional aspects of warfare.

The analysis is structured in four main parts. This introduction is followed by a short contextualisation to situate the analysis in the wider conversation about emerging technologies and the future of warfare (Part 2). Part 3 provides a short overview of the conflict so far, dividing it into six phases. Part 4 surveys the main elements of the conflict in Ukraine, outlining what emerging technologies have been present and critically assessing their role in the war. Part 5 delves into some implications for the future of warfare that can be understood from the dynamics analysed thus far, especially as they relate to the place of emerging technologies in future conflicts and their role in determining battlefield outcomes.

We argue that while some new technologies have come to characterise modern warfare, the Russo-Ukrainian conflict shows that many features of warfighting remain unchanged. Emerging technologies, such as AI and cheaper technological alternatives to traditional armaments, such as drones, are undoubtedly starting to change the battlefield and will play an increasingly larger role in future conflicts. Cyberspace and the globalised digital information space are bringing new actors and new means to exert influence, provide nations' armed forces with new tools, and make battlefields increasingly globalised and complex.

However, the conflict also shows that traditional aspects of warfare will not decrease in importance or be sidelined. Conflicts remain a contest of wills and adaptation, where ammunition supplies, the quantity of traditional armaments such as tanks, and both the number and quality of personnel and the logistical and organisational ability to bring all these elements to bear all remain the most important determinants of success. While technology is playing an increasing role in this equation, it remains unable to determine the outcome of a conflict on its own.

II. Contextualising the discussion on emerging technologies and the future of war

Research on war and its future is closely linked to the prevailing concerns of policymakers, geopolitical realities, socio-political norms, and predominant forms of conflicts at any given time. While technology has always been central to the discussion, over the last 20 years it has seen an uptick in the attention given to it as one of the most important harbingers of change in warfare. Reflecting the pace of unprecedented digital technological innovation since the 1990s, experts have predicted broad – sometimes revolutionary – changes to the character of war, and sometimes to its nature.[1] Largely driven by a revolution in information technologies, scholarship has identified and debated various "Revolutions in Military Affairs" (RMAs), or "disruptive or significant military change brought by the convergence of emerging 'next frontier' technologies, novel operational concepts and organisational force structures".[2] While some level of definitional ambiguity relating to emerging technologies remains, in the context of this paper emerging technologies are considered to be relatively novel technologies characterised by uncertainty, exhibiting fast growth, and displaying high disruptive potential.[3]

Technological innovations coupled with the lack of large-scale interstate conflicts, the rise of global competition through other means, and the global focus on counterterrorism and counterinsurgency have led to a large focus on "hybrid" forms of warfare. This has in turn led to an expectation that confrontation in the 21st century would largely take place below the threshold of overt war and would often be waged through surrogates – and increasingly through technological surrogates (such as long-range drones during the so-called "War on Terror" or AI-enabled disinformation activities more recently).[4] These analyses mirrored a world expecting war to become small, peripheral, and hybrid, as well as remote, precise, efficient, and less deadly. In this context, the place of technology as the key determinant of success and (mostly US) military advantage in 21st century battlefields was heavily emphasised. This led to extreme predictions such as that "future generations may come to regard tactical warfare as properly the business of machines and not appropriate for people at all ... direct human participation in warfare is likely to be rare".[5] In the mid-2010s the proliferation of personal computing, mobile phones, and the "Internet of Things", coupled with the increased digitalisation and connectivity of critical infrastructure, saw increased attention being given to "cyber war", and digital means of coercion more broadly.[6] However, some scholars did caution against overemphasising the RMA thesis and the role of technology in leading to disruptive changes to warfare. For example, one suggested instead that "21st century warfare will be mainly a continuation of a century-long increase in the importance of skill in managing complexity, not a revolutionary break with the past".[7] These scholars emphasised behaviour and adaptation as key variables determining technological efficiency and new technologies' subsequent impact on warfare. As such, they adopted a more human and human-processes-centric view of warfare, in which technology brings increased complexity to warfare and success is determined not by the technologies themselves, but by the ability both to navigate this complexity and protect oneself from it.

In recent years, the focus on technology in warfare scholarship has constantly increased.[8] Discussions surrounding technology and the future of warfare have since mostly focused on the role that AI will play in warfare. This has been largely driven by a considerable acceleration of AI-related scientific advances, as well as their permeation into everyday life through various products and applications. This has been further exacerbated by the resulting growing importance of technology – and a country's technology sector – to national security and the subsequent intensification of global geopolitical competition in the technology sphere.

Some have argued that this "AI-driven RMA" differs from previous ones, and that "a military-technology tsunami is on the way that may defy previous revolutions in military affairs".[9] For them, current ways of warfare may rapidly become obsolete, driven by advances in AI, the increased importance of dual-use technology in defence innovation and renewed global geopolitical competition.[10] Expert attitudes towards the effects of AI on warfare have broadly fallen into three categories: enthusiasm, denial and pragmatism.[11] Enthusiasts maintain that the adoption of AI will dramatically alter the character of warfare, deeply altering its strategic, operational, and tactical levels and – in time – potentially altering its very nature.[12] In fact, AI's qualitative difference from other technologies, mostly in its ability to power increasing autonomy in an increasing number of weapons functions, has given new wind to the expectation that technology may one day replace or take over from humans in warfare. Pragmatists predict that some levels of change will influence the character of warfare, albeit in a more limited, less revolutionary way. For their part, deniers maintain that technical and organisational hurdles remain too high and limit the usefulness and disruptive potential of military AI. In this view, AI remains too immature and unreliable for the realities of war.[13] All in all, the pervasive view among major militaries remains that AI will confer key advantages on successful adopters, facilitating decision-making superiority and increased operational speed and mass. This has had the net effect of making the study of war increasingly technology centric, whereby proponents have even suggested that technology (in this case AI) might even be the solution to some of the most human aspects of warfare, such as ensuring respect for international humanitarian law (IHL) or the reduction of civilian casualties.[14]

There is now a risk that the rapid development of a disruptive technology such as AI leads to an overestimation of its potential in warfare and its subsequent accelerated application in various aspects of the military domain, often disregarding or minimising its potential associated risks. This is all largely based on the previously mentioned still unproven expectations of efficiency gains and revolutionary advantages conferred on successful adopters. As one of the first major interstate conflict in the "age of AI" and dual-use technologies – at least in modern terms – the war in Ukraine is an opportunity to gauge their impact on warfare. This, of course, is done with the understanding that there is a limit to the generalisability of conclusions extrapolated from a single – still ongoing – conflict.

Still, an emergent body of literature is addressing lessons from the conflict for the future of warfare. Mirroring the global attention on AI, the presence of drones and various AI applications has skewed some analyses towards overestimating and overstating the place these "new" elements have in the war. In contrast, the undeniable brutality and scale of the war, as well as the seemingly unending flow of images of trenches, mud and burnt-out vehicles, have also led to a slew of analyses pointing to war's seemingly unchanged character.[15] The analysis presented in this paper is an addition to this debate, seeking to strike a balance by highlighting both the new and the old features of war and conflict. In so doing, it aims to promote the idea that predictions of the impact that AI and other emerging technologies will have on warfare must be rooted in the analysis of their actual use in the adversarial conditions present in conflicts, and that careful observation of the war in Ukraine is an opportunity to do so.

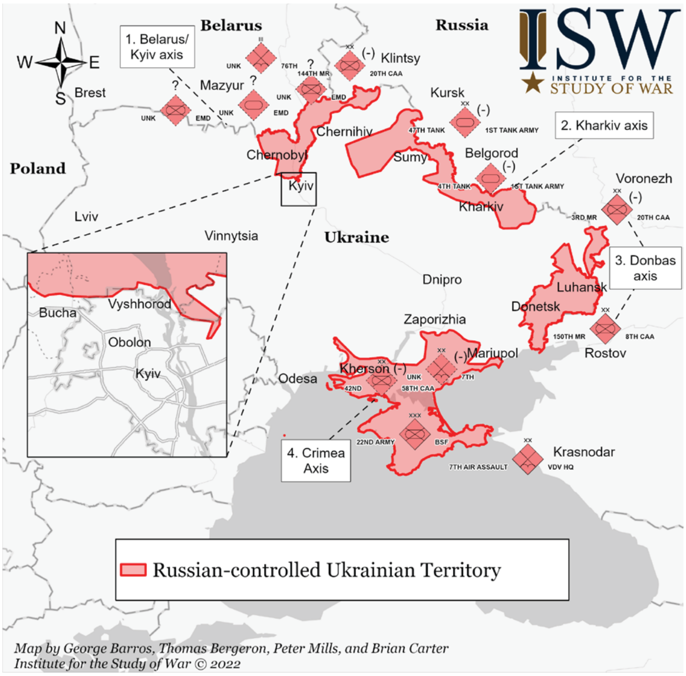
III. A war in different phases

It is important to note that, as of March 2024, the war in Ukraine can be roughly divided into six phases. Each phase presents some distinct features that both influence the presence and impact of emerging technologies and are influenced by them. It is therefore worth briefly describing each phase.

Phase 1: February-April 2022: initial Russian invasion

The first phase of the war saw 200,000 Russian troops cross the Ukrainian border to conduct a multipronged attack along four axes in the south, east and north of the country. The logic behind this multifront attack was to quickly overrun Ukraine in a rapid offensive, occupy its main cities and ports, take Kyiv, and overthrow President Zelensky's government. The under-estimation of the strength of Ukrainian forces, poor planning, flawed assumptions, and logistical problems are only some of the issues that plagued Russian forces during this first phase in which Russia failed to achieve most of its objectives. Ukrainian forces and a large number of civilian irregulars were able to capitalise on these factors and inflict heavy personnel and material losses on Russian forces. At the end of the first stage in April 2022, US sources estimated that 5,000 Russian soldiers had been killed.[16] However, Russian forces where able

Figure 1: Russian territorial control as of 27 February 2022[17]



Map by George Barros, Thomas Bergeron, Peter Mills, and Brian Carter
Institute for the Study of War © 2022

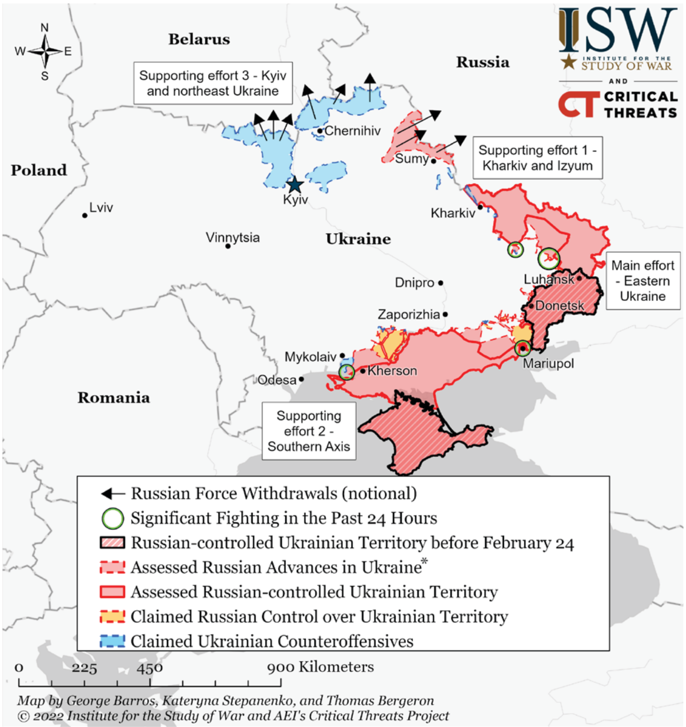
Institute for the Study of War and AEI's Critical Threats Project

to make substantial gains in the south of the country, where operational speed and the more appropriate assessment of Ukrainian defences resulted in more Russian objectives being achieved.[18]

Phase 2: April-June/July 2022: from manoeuvre to positional war

As the logistical overstretch of invading along so many axes quickly became unsustainable and the strength of Ukraine's defence obvious, Russia refocused its efforts and narrowed down its goals in the east of Ukraine, thus starting the second phase of the war in April 2022. This phase was characterised by the use of heavy artillery to flatten cities and Ukrainian defensive positions in the east, and incremental gains, attrition, and heavy casualties on both sides. Ukrainian forces, struggling in the face of Russian artillery barrages, lost at least 200 men per day as the phase peaked in June.[19] While Russian losses are uncertain, August 2022 estimations show crippling damage, with US and Ukrainian sources putting the casualty count at between 50,000 and 80,000, and three to four thousand armoured vehicles destroyed.[20] Despite the loss of cities such as Sieverodonestk and Lysychansk, Ukrainian forces avoided an encirclement of their forces in the east and forced Russian forces to reduce their territorial ambitions away from Kyiv and focus on conquering

Figure 2: Russian territorial control as of 5 April 2022[21]


N
W
E
S
Belarus
Russia
ISW
INSTITUTE FOR THE STUDY OF WAR
AND
CT CRITICAL THREATS
Supporting effort 3 - Kyiv and northeast Ukraine
Chernihiv
Sumy
Supporting effort 1 - Kharkiv and Izyum
Poland
Kyiv
Kharkiv
Lviv
Vinnytsia
Ukraine
Main effort - Eastern Ukraine
Luhansk
Dnipro
Donetsk
Zaporizhia
Mykolaiv
Kherson
Mariupol
Odesa
Romania
Supporting effort 2 - Southern Axis
Russian Force Withdrawals (notional)
Significant Fighting in the Past 24 Hours
Russian-controlled Ukrainian Territory before February 24
Assessed Russian Advances in Ukraine*
Assessed Russian-controlled Ukrainian Territory
Claimed Russian Control over Ukrainian Territory
Claimed Ukrainian Counteroffensives
0 225 450 900 Kilometers
Map by George Barros, Kateryna Stepanenko, and Thomas Bergeron
© 2022 Institute for the Study of War and AEI's Critical Threats Project

Institute for the Study of War and AEI's Critical Threats Project

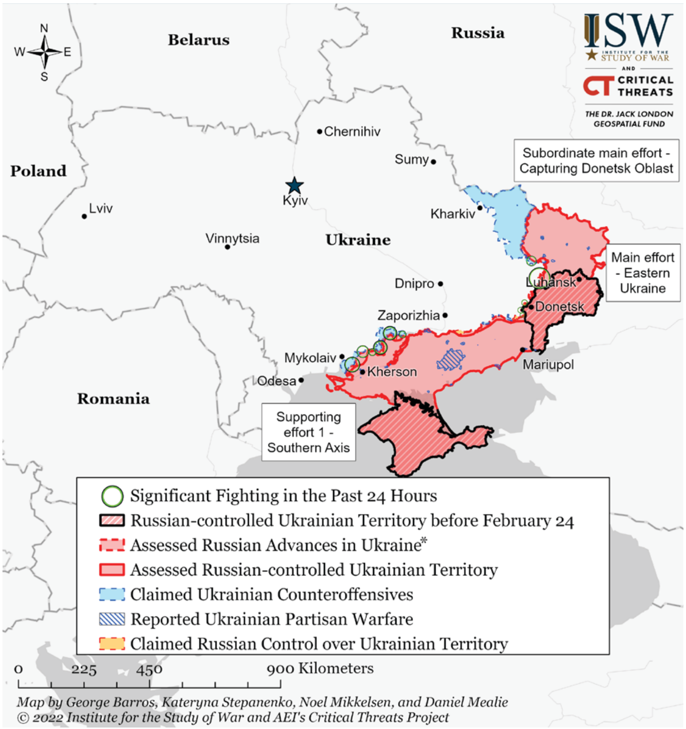
new territories in the Donbas region.[22] This second phase of the war was also characterised by the delivery of increasingly advanced weaponry to Ukraine from the West, especially longer-range guided munitions. Ukraine was also proficient at targeting Russian forces as they massed to attempt river crossings in the east. In tandem with destroying road and rail infrastructure, including bridges, this was a key element of slowing Russia's advance.

Phase 3: September-November 2022: first Ukrainian counter-offensive

Relying on strategic surprise and deception, as of September 2022 a third phase of the conflict featuring a Ukrainian counter-offensive led to large territorial gains for Kyiv. In June-July 2022 Russia undertook an operational pause to replenish supplies (both material and personnel). Ukraine took this time to do the same and began signalling its intent to start a counter-offensive in the south of the country. As Ukraine hit key logistical and supply targets deep behind Russian lines – sometimes as far as Crimea – Russia moved much of its force to the south in preparation for the Ukrainian offensive.

In September 2022 Ukrainian forces moved against Russian positions around the southern city of Kherson. By mid-September the reality of a Ukrainian tactical

Figure 3: Russian territorial control as of 20 September 2022[23]


N
W
E
S
Belarus
Russia
ISW
INSTITUTE FOR THE STUDY OF WAR
AND
CRITICAL THREATS
THE DR. JACK LONDON GEOSPATIAL FUND
Chernihiv
Sumy
Poland
Kyiv
Lviv
Kharkiv
Subordinate main effort - Capturing Donetsk Oblast
Vinnytsia
Ukraine
Dnipro
Luhansk
Main effort - Eastern Ukraine
Donetsk
Zaporizhia
Mykolaiv
Kherson
Mariupol
Odesa
Romania
Supporting effort 1 - Southern Axis
○ Significant Fighting in the Past 24 Hours
▨ Russian-controlled Ukrainian Territory before February 24
▨ Assessed Russian Advances in Ukraine*
🟥 Assessed Russian-controlled Ukrainian Territory
▨ Claimed Ukrainian Counteroffensives
▨ Reported Ukrainian Partisan Warfare
▨ Claimed Russian Control over Ukrainian Territory
0
225
450
900 Kilometers

Map by George Barros, Kateryna Stepanenko, Noel Mikkelsen, and Daniel Mealie
© 2022 Institute for the Study of War and AEI's Critical Threats Project

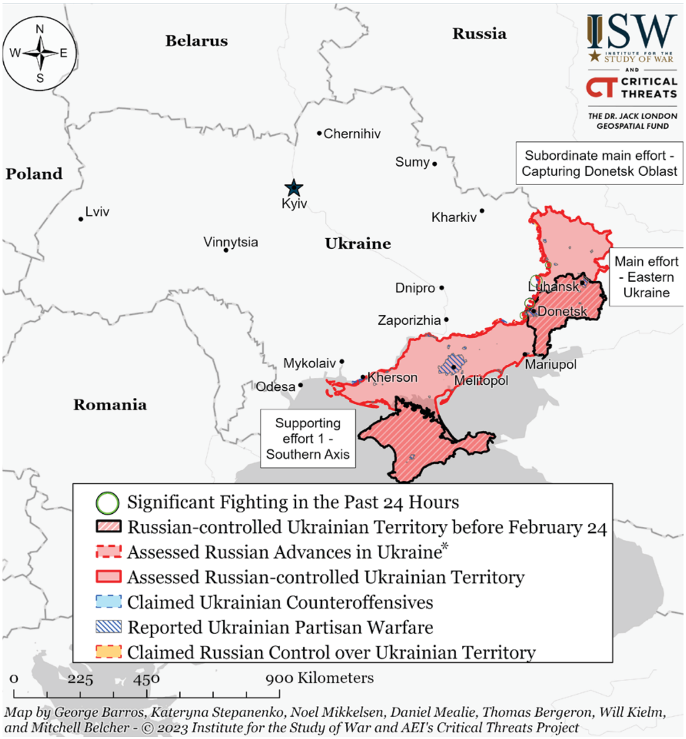
Institute for the Study of War and AEI's Critical Threats Project

surprise became evident as Ukraine launched a more ambitious, simultaneous counter-offensive in the north of the country, around Kharkiv. In a very short period of time Ukraine – benefitting from its deception and Russia's repositioning of its troop in the south – liberated vast swathes of territory, essentially liberating almost all of Kharkiv oblast, an area of approximately 6,000 km2, and nullifying Russia's wartime gains in the area.[24] This led to Ukraine regaining 54% of all the territory lost since February 2022.[25] In November 2022 Ukraine also regained control of the city of Kherson. Unable to mount a successful counter-offensive of its own, Russia unleashed a campaign to destroy Ukraine's critical energy infrastructure with the use of long-range ballistic and cruise missiles, as well as Iranian-acquired Shahed 136 drones.[26]

Phase 4: December 2022-June 2023: stabilisation of the front and the battle for Bakhmut

Following Ukraine's counter-offensive, the front line barely moved between winter 2022-23 through to spring 2023. At this stage the war settled once more into a bloody positional war of attrition. The main Russian thrust centred around the city of Bakhmut, principally undertaken by the so-called Wagner Group, which branded itself as Wagner Private Military Company (PMC). The battle for

Figure 4: Russian territorial control as of 20 May 2023[27]


N
W
E
S
Belarus
Russia
ISW
INSTITUTE FOR THE STUDY OF WAR
AND
CRITICAL THREATS
THE DR. JACK LONDON GEOSPATIAL FUND
Chernihiv
Sumy
Poland
Kyiv
Subordinate main effort - Capturing Donetsk Oblast
Lviv
Kharkiv
Vinnytsia
Ukraine
Main effort - Eastern Ukraine
Luhansk
Dnipro
Donetsk
Zaporizhia
Mykolaiv
Mariupol
Kherson
Melitopol
Odesa
Romania
Supporting effort 1 - Southern Axis
Significant Fighting in the Past 24 Hours
Russian-controlled Ukrainian Territory before February 24
Assessed Russian Advances in Ukraine*
Assessed Russian-controlled Ukrainian Territory
Claimed Ukrainian Counteroffensives
Reported Ukrainian Partisan Warfare
Claimed Russian Control over Ukrainian Territory
0
225
450
900 Kilometers

Map by George Barros, Kateryna Stepanenko, Noel Mikkelsen, Daniel Mealie, Thomas Bergeron, Will Kielm, and Mitchell Belcher - © 2023 Institute for the Study of War and AEI's Critical Threats Project

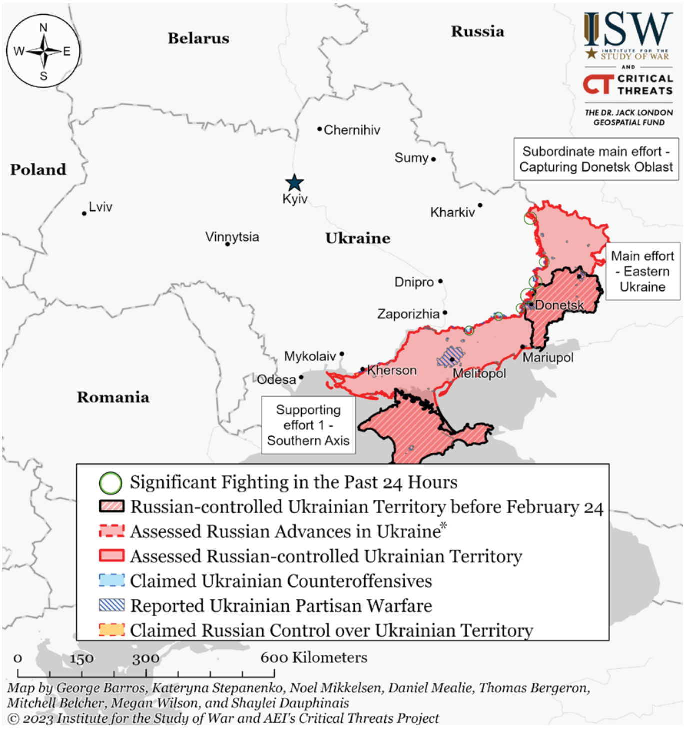
Institute for the Study of War and AEI's Critical Threats Project

the city pinned down both forces, eventually falling to Russian occupation in May 2023. With Wagner PMC and Russian forces utilising brutal “meatgrinder offensives”, estimates put casualties at 100,000 for Russia and 20,000 for Ukraine in the battle for Bakhmut alone. [28] The centrality of Bakhmut in this phase of the war also speaks to the increase prevalence of Wagner PMC forces in the conflict and the role of their leader, Yevgeny Prigozhin. A short episode of political instability was triggered by the mutiny of some elements of Wagner PMC, which eventually led to the death of Prigozhin. This phase of the war also saw the continuation of the Russian campaign against Ukrainian infrastructure using a variety of means, including Shahed drones, cruise missiles, ballistic missiles and the so-called Kinzhal air-launched hypersonic missile.

Phase 5: June-December 2023: second Ukrainian counter-offensive

Wars of attrition favour the party that can sustain human and capability losses the longest.[29] With this reality in mind, the pressure increased on Ukraine to regain the initiative and mount a successful counter-offensive. While pinning down Russian forces around Bakhmut, Ukraine therefore spent much of the war’s previous phase gathering Western armaments, including for the first time Western main battle tanks, and training its troops for a large-scale, combined arms offensive in the summer of 2023. In the time needed to prepare for this

Figure 5: Russian territorial control as of 2 November 2023[30]


N
W
E
S
Belarus
Russia
ISW INSTITUTE FOR THE STUDY OF WAR
AND
CT CRITICAL THREATS
THE DR. JACK LONDON GEOSPATIAL FUND
Chernihiv
Sumy
Poland
Subordinate main effort - Capturing Donetsk Oblast
Kyiv
Lviv
Kharkiv
Vinnytsia
Ukraine
Main effort - Eastern Ukraine
Dnipro
Donetsk
Zaporizhia
Mykolaiv
Kherson
Melitopol
Mariupol
Odesa
Romania
Supporting effort 1 - Southern Axis
○ Significant Fighting in the Past 24 Hours
▨ Russian-controlled Ukrainian Territory before February 24
▨ Assessed Russian Advances in Ukraine*
🟥 Assessed Russian-controlled Ukrainian Territory
▨ Claimed Ukrainian Counteroffensives
▨ Reported Ukrainian Partisan Warfare
▨ Claimed Russian Control over Ukrainian Territory
0 150 300 600 Kilometers
Map by George Barros, Kateryna Stepanenko, Noel Mikkelsen, Daniel Mealie, Thomas Bergeron, Mitchell Belcher, Megan Wilson, and Shaylei Dauphinais
© 2023 Institute for the Study of War and AEI's Critical Threats Project

Institute for the Study of War and AEI's Critical Threats Project

offensive, divisions between US and Ukrainian planners, the lessons of Ukraine's first counter-offensive, and the positional nature of the war's previous phase allowed Russian forces to prepare for Ukraine's summer offensive far better. At the initiative of General Surovikin, the Russian armed forces built vast networks of layered, deeply entrenched defences in southern Ukraine, the eventual main axis of Ukraine's thrust.[31] The counter-offensive therefore largely failed to achieve its objectives (to liberate Kherson and Zaporizhzhia oblasts and reach the Sea of Azov), with little to show for five months of operations.

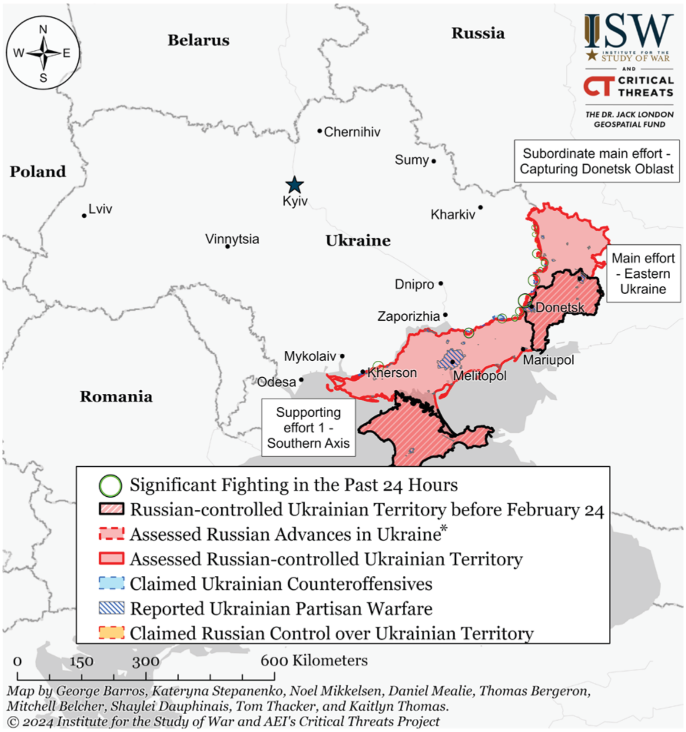
Russia's deep and elastic defences and the absence of any Ukrainian technological edge or numerical advantage over Russian forces rendered the battlefield extremely lethal for large-scale operations, especially for mechanised brigades. The key armoured components of the Ukrainian forces were often destroyed at distances of up to 5 km by Kamov 52 Alligator helicopters that took advantage of the local geography to perform their anti-armour role precisely as intended during their design phase in the late 1980s and early 1990s. In the face of mounting casualties and equipment losses due to extremely dense minefields, a dilution of force density over three axes, and the ever-present drones and endless trench networks, Ukraine quickly abandoned a Western-style large-scale mechanised manoeuvre to return to its early war small-group infantry assault tactics.[32]

This phase of the war also saw the escalation of activity in the Black Sea. Despite, Ukraine's lack of an operational navy, but thanks to the innovative use of unmanned surface vessels (USVs) and long-range unmanned aerial vehicles (UAVs), Ukrainian forces achieved several successful strikes on Russia's Black Sea fleet and its headquarters in Sevastopol.[33] The attacks forced Russia to relocate parts of its fleet and effectively denied it freedom of navigation in the Black Sea.[34]

Phase 6: December 2023-present: culmination of Ukrainian counter-offensive, stalemate and Russia regains the initiative

As of early 2024, the war largely reached a stalemate once more as both forces recovered from the counter-offensive, but the momentum has currently shifted towards Russia.[35] Indeed, the former commander of Ukraine's forces stated that "just like in the First World War we have reached the level of technology that puts us into a stalemate".[36] Benefitting from an asymmetry of capabilities and troop numbers, Russia has managed to regain the initiative by conducting successful offensives such as in Avdiivka. Despite reportedly losing up to 1,380 men, 55 tanks, and 120 armoured fighting vehicles in one day of combat alone,[37] Russia's military capacities and ability to absorb personnel losses far exceed those of Ukraine in this combat phase. With Western – especially US – support slowly waning, the present stalemate therefore increasingly favours the Russian position. As Ukraine prepares for what is certainly to be a decisive year for the war, force generation efforts have taken centre stage, as Ukraine's inability to sustain the war at the current level of human attrition comes sharply into focus.[38] It remains to be seen the extent to which Ukraine will be able to regenerate its forces while fending off Russian offensive pressures.

Figure 6: Russian territorial control as of 14 March 2024[39]


N
W
E
S
Belarus
Russia
ISW INSTITUTE FOR THE STUDY OF WAR
AND
CT CRITICAL THREATS
THE DR. JACK LONDON GEOSPATIAL FUND
Chernihiv
Sumy
Poland
Subordinate main effort - Capturing Donetsk Oblast
Lviv
Kyiv
Kharkiv
Vinnytsia
Ukraine
Main effort - Eastern Ukraine
Dnipro
Donetsk
Zaporizhia
Mykolaiv
Mariupol
Kherson
Melitopol
Odesa
Romania
Supporting effort 1 - Southern Axis
○ Significant Fighting in the Past 24 Hours
▨ Russian-controlled Ukrainian Territory before February 24
▭ Assessed Russian Advances in Ukraine*
▭ Assessed Russian-controlled Ukrainian Territory
▭ Claimed Ukrainian Counteroffensives
▨ Reported Ukrainian Partisan Warfare
▭ Claimed Russian Control over Ukrainian Territory
0
150
300
600 Kilometers
Map by George Barros, Kateryna Stepanenko, Noel Mikkelsen, Daniel Mealie, Thomas Bergeron, Mitchell Belcher, Shaylei Dauphinais, Tom Thacker, and Kaitlyn Thomas.
© 2024 Institute for the Study of War and AEI's Critical Threats Project

Institute for the Study of War and AEI's Critical Threats Project

IV. Old and new: technological realities of the battlefield

A. Drones

The war in Ukraine shows that drones – of various levels of sophistication, autonomy and types of functions – have become essential element of modern warfare. This war shows that when successfully integrated into battlefield tactics and as part of mature concepts of operations, drones can confer asymmetric advantages to outgunned armies and provide cost-effective and sophisticated intelligence, reconnaissance, and strike capabilities.

In fact, the conflict has seen the deployment of the widest array of drone types in a conflict to date, featuring everything from military-grade medium-altitude long-endurance drones such as the Turkish TB2, to loitering munitions such as the US Switchblade, to commercial DJI quadcopters and home-made first-person view (FPV) drones.[40] Ukraine's armed forces have been touted as having been both quicker and more effective in their understanding of this reality and in the development and deployment of various drone capabilities.

Early in the conflict the Turkish TB2 was a staple of Ukraine's resistance on some fronts. TB2s were effective in slowing down Russian progress on the Zhitomir front, providing surveillance and cost-effective air support in the absence of conventional combat-aircraft-enabled air support. For example, by exploiting poor Russian mechanised forces deployment tactics, TB2s proved instrumental in the destruction of Russian mechanised units and air defences. Moreover, they served as an effective Ukrainian propaganda tool, with video feeds of successful Ukrainian strikes on Russian troops and tanks circulating on social media and galvanising support.[41]

More importantly, however, Ukraine has been particularly adept at utilising small, often off-the-shelf commercially available drones, such as Chinese-made DJI Matrice and Mavic drones, often crowdsourced and modified to carry and deliver explosives.[42] In the early days of the war these drones were largely used to drop grenades and other such small ordinance on Russian infantry and materiel.[43] Later phases of the war, however, have seen the increased prevalence of these drones being used as Kamikaze drones piloted in FPV to strike both infantry and armoured vehicles.[44] This has given Ukraine both an incredibly cheap and effective alternative to conduct strikes, and a means to engage in psychological warfare.[45]

Because Russia is often able to fire up to five times as many shells than Ukraine, drones have by and large become Ukraine's alternative to narrow the gap.[46] However, as drones remain limited in their maximum possible payload, their largest impact has been their use in reconnaissance and guiding artillery fire.[47] It is now estimated that drone reconnaissance supplies Ukrainian forces with

86% of all identified targets.[48] Drones are furthermore conferring increased battlefield awareness on small infantry teams and individual soldiers, so much so that it is now inconceivable to conduct operations without at least one drone in the sky.[49] While this has assisted operations and made artillery targeting more accurate, it has made the battlefield immensely transparent and lethal, ensuring that there is truly nowhere to hide.[50] The result has been the increased difficulty to concentrate force, achieve surprise and conduct offensive operations.[51]

Drones have been of such importance to the war effort that Ukraine has directed national efforts to acquiring drones, developing homegrown capabilities and training pilots.[52] Indeed, one of the most important lessons learned through Ukraine's experience is not only a military one linked to the use of the drones themselves, but also *how* the country has acquired and developed its various drones. Ukraine has been able to successfully leverage the global "big tech" ecosystem, its civilian commercial technology sector, and domestic start-ups, NGOs, and even individual civilians for its "drone war".

To this effect, Ukraine successfully shortened the loop between prototyping, experimenting, testing, producing and fielding drones, as well as streamlining procedures to provide the armed forces with drone technologies. This has enabled it to substantially increase its production and facilitated the fielding of drones that more directly meet the needs of field units.[53] While only seven companies were making drones in Ukraine before the war, there are now up to 200 making over 300 types of drones.[54] In 2024 Ukraine is set to produce 1 million FPV drones.[55]

As the culmination of these efforts, Ukraine has created a new, separate branch of its military focused entirely on unmanned systems. The novel Unmanned Systems Force will focus on "improving Ukraine's work with drones, creating special drone-specific units, ramping up training, systemising their use, increasing production, and pushing innovation".[56]

Ukraine has notably been able to leverage its creativity and efficient development, testing, and repurposing of dual-use technologies in the development, modification, and deployment of drones to greatest effects in its naval efforts. Lacking an operational navy from the very beginning of the conflict, but still needing to engage Russia in the Black Sea, both to threaten Crimea and protect its own shipping lanes, Ukraine developed homegrown naval drones or USVs. A string of attacks on targets far from the south-west Ukrainian coast – in and around Sevastopol in Crimea, and even further across the Black Sea to the Russian port of Novorossiysk – show that these USVs have the capability to evade Russian defences in the country's waters, pose serious threats to Russian naval assets, and restrict Russian freedom of navigation.[57]

This is all the more notable because these USVs comprise a homegrown mix of commercial technology laden with explosives. They seem to have been originally constructed with a Canadian jetski engine, a Starlink satellite antenna and an electrical-optical infrared imaging system.[58] These USVs represent a perfect example of the use of off-the-shelf, cheaper technological alternatives to rebalance the power dynamics on the battlefield and threaten much more advanced and expensive systems such as frigates and cruisers – and even Russian flagships.[59] Using a combination of USVs and missiles, Ukraine has reportedly destroyed 40% of Russia's naval tonnage in the Black Sea.[60]

Russia's performance relating to the use of all types of drones is more uneven, but should not be dismissed. The early phases of the war were characterised by the lack of the widespread use of UAVs by the Russian side.[61] Some experts indeed argue that Russia's lack of drone usage for intelligence, surveillance and reconnaissance contributed to its early invasion blunders, notably due to the lack of situational awareness resulting from the absence of drones.[62] This is particularly surprising in light of Russia's US$ 9 billion investment in UAV technology since 2014, putting in focus the existence of a wide gap between the country's unmanned and autonomous warfare aspirations and battlefield realities.[63]

Russia in fact initially seemed to be mainly using relatively short-range, remote-controlled UAVs and very few longer-range combat UAVs of its own making.[64] Russian drone warfare efforts might have also been hampered by Russia's rigid command structure, which requires soldiers to obtain senior approval for strikes, often nullifying the advantage conferred by the decentralised, mobile and flexible use of drones.[65] Ukraine has been more successful at adopting such tactics.

Additionally, failure to create similar conducive conditions to those of Ukraine for the successful rapid development and deployment of various drone capabilities further hampered Russia's track record.[66] Russia's cumbersome and centralised bureaucracy coupled with a lack of government leadership and a domestic environment unfriendly to bottom-up innovation are partly to blame.[67]

While Ukraine's advantage was more pronounced in the first three phases of the war, Russia has now largely caught up, especially in the field of FPV drones. Its efforts remain more reactive than active, but it has adopted many of Ukraine's tactics with regard to drones, using a deadly combination of its Orlan-10 surveillance and Lancet drones, as well as the Iranian-made Shahed 136, coupled with superior electronic-warfare (EW) capabilities, against Ukraine's drones.[68] As one report puts it, "Ukraine has consistently out-innovated Russia with commercial technologies and software, but Russian forces have quickly adapted and emulated Ukrainian successes".[69] While Russia conducted half as many FPV strikes on Ukraine as the latter conducted on Russian targets in September 2023 (approximately 200 versus 400), current strikes number are now essentially equivalent (about 1,000 per month).[70]

However, it is important to balance out the overall discussion surrounding the importance of drones and their impact on the war. In fact, the success of drones and their impact on determining battlefield outcomes have been highly dependent not only on the drones themselves, but their conditions of use and the realities of their operational environments.

To some extent, Ukraine's early successes were mostly a result of the failures and mistakes of Russian forces and the tactics they adopted, coupled with their failure to use drones themselves. This created a permissible environment for drones to be used to their maximum effect. This is particularity true of the TB2s, whose limited successes in the first phase of the war, for example, can be attributed to the fact that Russia's armoured divisions lacked infantry support, air support, effective air defences, and effective EW capabilities, and suffered from overstretched supply lines and faulty tactics.[71]

As the battlefield became more static in the second phase of the war, supply lines shorter and easier to manage, EW and air defences more efficient, and Russian strategy shifted from mobile operations to artillery barrages, the effect of drones in advancing Ukrainian objectives was more muted.[72] The Russians became more adept at shooting down Ukrainian drones. Slow moving and low flying, they became vulnerable to the better organised and entrenched Russian air defences. While TB2 drones presented a low-cost airpower alternative to inflict disproportionate damage earlier on in the conflict, in the second phase of the war their vulnerability made them – at US$ 2-10 million apiece – a costly loss.[73]

Perhaps due to this cost, small, cheap drones have remained most useful in their "enabling" roles to reduce the time-to-trigger for artillery, providing battlefield awareness, guiding artillery strikes and as accurate single-use munitions themselves.[74] With more entrenched Russian forces and more efficient Russian EW, the survivability of UAVs is now relatively low. It is estimated that around 90% of all UAVs utilised are lost, with an average life expectancy of three to six flights, depending on the model.[75] It is further estimated that Ukraine is losing up to 10,000 drones per month.[76] Additionally, while sourcing drones from civilians and technology start-ups (even if centralised, incentivised and facilitated through government programmes such as the Brave1 accelerator[77]) enabled Ukraine to gain an early advantage in the drone war, there is also a notable downside. While this has enabled these drones to be cheap and numerous – vital for a resources-strapped nation under siege – and has conferred on Ukraine some asymmetric advantages, some of their cheaply made parts have been the cause of failures and malfunctions.[78] This, coupled with the lack of standardisation between the many types of drones that units have available to them, has sometimes complicated drone operations and reduced their efficiency.[79]

Drones remain an essential aspect of operations for both armed forces, but Russia and Ukraine have reached a relative technological match.[80] Although they have transformed the way in which infantry operations are conducted by increasing the transparency of the battlefield, at this stage drones are unlikely to provide either side with the breakthrough they need. The war in

Ukraine demonstrates that drones have become a key weapon of modern battlefields, yet they should not be seen as game changers and determinants of battlefield outcomes in isolation. The disruptive effect of drones depends on their operational concept and their integration with other weapons systems. At present, outgunned and outmanned, Ukraine requires more tanks, armoured vehicles, spare parts, artillery pieces, ammunition and manpower, not only drones, to be able to reclaim the initiative and conduct effective offensive and defensive operations.[81]

B. What role for AI?

AI-enabled emerging technologies have made sporadic appearances throughout the conflict and have become a key talking point of the war in Ukraine.[82] In fact, the war has very much acted as a testbed for many of the AI applications whose potential militarisation experts have been predicting in recent years. More importantly, it is not only their presence that is of note, but the fact that their successful operationalisation has been touted as an important contributor to Ukraine's relative successes. In the military domain, AI can be broadly characterised as an analytical enabler, a disruptor or a force multiplier.[83] As an analytical enabler, AI can help with the data-heavy aspects of warfare by collecting, fusing, and analysing immense troves of data at scale and at great speeds. As a disruptor, various generative AI techniques can now both produce and help spread extremely believable media, be it text, image or video, to be used in disinformation campaigns and cognitive warfare.[84] As a force multiplier, AI is key to enabling the ever-increasing autonomy of various weapons systems. In Ukraine, AI has been present in all three of these functions.

AI as an analytical enabler

As an analytical enabler, AI has reportedly powered much of the intelligence, reconnaissance and targeting done by Ukraine. Perhaps the greatest contribution that AI has made to the Ukrainian war effort lies in its power to gather, analyse, and fuse data to create a real-time operational picture of the battlefield that contributes to assisting and accelerating the targeting process. In this way, the use of AI can accelerate the observe, orient, decide, act (OODA) loop process.[85]

For instance, Ukrainian forces have made use of an "Uber-like" application to innovate and speed up their artillery targeting. Named "GIS Arta", it is a decentralised and distributed command-and-control application that is able to process data from drones, smartphones, rangefinders, and connected artillery computer. Once a target is identified, the application distributes the fire command to the closest and most appropriate platform to carry out a strike. This has reduced the "call to trigger time" almost ten-fold, significantly increased the accuracy of Ukrainian artillery, and made it possible for fewer and more mobile artillery pieces to be effective tools against a numerically superior adversary.[86]

Other such platforms, such as Ukraine's homegrown DELTA battle-management software, have similarly been developed and used to leverage the power of data. Ukrainian forces upload information about Russian troops gathered from sources ranging from drone footage to human intelligence, and the app displays this information on a map of the country.[87] While this remains difficult to verify, Palantir CEO Alex Karp also claimed that his company was responsible for "most of the targeting" in Ukraine. Early in the war, Palantir reportedly offered its products to Ukraine free of charge.[88] Although their real capabilities remain secretive, Palantir's AI-enabled services utilise similar technology to gather and fuse various sources of intelligence, and subsequently suggest options for commanders.[89]

While it is difficult to know the exact mix of platforms, systems, and software utilised by Ukraine's armed forces and gauge their real impact, one thing is clear: Ukraine has understood the necessity of tapping into today's data-rich battlefields. This has been powered by the sheer amount of available data, from the vast number of digital devices (mostly commercial) capturing images, audio, and videos of the war, to the increased prevalence of open-source intelligence. Each individual – both civilian and military – equipped with a smart phone effectively has now become a sensor. Ukrainian authorities have, for example, opened a Telegram channel receiving tens of thousands of messages per day where citizens can send videos and photos of Russian troops and materiel, providing information that complements that of Ukrainian intelligence-gathering activities.[90] Citizens can also report Russian troop movements via the national Diia app.[91] Ukraine has also utilised other AI applications, such as natural language processing (NLP), notably thanks to AI company Primer, which utilises AI that uses its algorithms to listen in on intercepted Russian communications and automatically translate and highlight relevant information for Ukrainian forces in a searchable text database.[92]

For its part, Russia's much-touted "battlefield AI" seems to be relatively missing from the battlefield.[93] While since 2020 the Russian Ministry of Defence has been focusing heavily on military applications of AI, there has been little evidence of Russian uses of AI in military decision-making or in C4ISR in Ukraine.[94] International sanctions preventing Russian access to Western components coupled with a brain drain and the fact that Russia's nascent domestic AI industry remains far behind its near-peer competitors such as the United States and China may all contribute to this.[95] The Russian armed forces' aspiration for unmanned and automated warfare therefore seems to be at odds with the realities on the ground.[96] The main feature in the conflict on the Russian side has predominantly been characterised by the use of legacy equipment, "dumb bombs", and heavy artillery barrages, not to mention extremely high casualty rates.

AI as a force multiplier

The conflict has not only accelerated the prevalence of drones in modern warfare, as previously seen, but it has clearly also accelerated the drive for their increased autonomy. Driven both by the highly contested nature of the electro-magnetic spectrum and ensuing constant communication breakdowns between drones and pilots, and the desire to accelerate targeting, both Russia and Ukraine have sought to automate various aspects of drone engagements. This has resulted in a real arms race to field drones with ever-increasing levels of AI-enabled autonomy in both target selection and engagement.[97] Ukraine's minister for digital transformation, Mykhailo Fedorov, went so far as to claim that autonomous drones are both logical and inevitable.[98]

While the levels of AI-driven autonomy of any given capability are inherently difficult to ascertain, reports from both the Russian and Ukrainian sides seem to show that we are edging closer to fully fledged autonomous weapons systems that can select and engage targets fully autonomously.[99] Ukraine's Saker Scout drone, for example, which can find, identify and attack 64 different types of Russian military objects autonomously, reportedly has been used in a "human-out-of-the-loop" way to attack Russian targets when radio jamming or interference prevented operator control.[100] While information on Russian weaponry is a more closely guarded secret, a new variant of the highly effective Russian homegrown loitering munition Lancet is reported to be able to fly in swarms and find and engage targets autonomously.[101] This growing autonomy, coupled with lowering unit costs, and a clear desire to employ drones such as the Shahed 136 en masse to saturate defences have set the stage for the future employment of swarms. A swarm of drones can be defined as "multiple unmanned platforms and/or weapons deployed to accomplish a shared objective, with the platforms and/or weapons autonomously altering their behaviour based on communication with one another".[102] While "true" swarming remains elusive for now, the individual elements needed in a war context are starting to emerge, and the conflict is setting the premise that could lead to its eventual realisation. [103]

AI as a disruptor

AI has also shown some promise as a disruptor in war. Indeed, while its contributions to battlefield outcomes have been relatively limited, the presence of deepfakes and coordinated disinformation efforts show an appetite to militarise these AI applications.

Generative adversarial networks have been used very early in the conflict through the creation of deepfakes of both presidents Zelensky and Putin.[104] Deepfakes have been the subject of much literature in the past few years due to their disruptive potential, but also for their possible militarisation.[105] Although of low quality and promptly debunked by Ukrainian authorities and the public, Zelensky's deepfake calling on Ukraine's citizen to drop their weapons in March 2023 showed how rapidly a technology that did not exist ten years earlier could be militarised and have an effect in conflict. Ukraine then retaliated with the diffusion of a hyper-realistic deepfake of Vladimir Putin calling for mass mobilisation and declaring martial law after some Russian TV and radio channels were hacked in early June 2023.[106]

As recent advances in generative AI have greatly accelerated in the past year alone (2023), it is safe to say that these capabilities will enable the creation of content indistinguishable from real content, making them increasingly disruptive.[107] Ukrainian forces have similarly used facial recognition technology from the US company Clearview AI to identify dead Russian soldiers and subsequently contact their families as part of propaganda efforts.[108] Coordinated disinformation and misinformation campaigns have been a feature of the conflict, instrumentalising social media algorithmic dynamics to spread war narratives. As part of information warfare, these dynamics will be further discussed in Part D of this section.

While present in various forms, AI-enabled emerging technologies have not been a panacea, even for their most adept users. Even though Ukraine has successfully used its technology sector and has been better able to leverage the cutting edge of AI-enabled warfare applications, the grim realities of war remain. For all their abilities to increase situational awareness by gaining AI-generated insights into the battlefield, Ukraine's forces have still suffered from communication breakdowns, chaotic withdrawals or friendly fire accidents.[109]

Importantly, the networking of the battlefield is reportedly much less automated than has been assumed, with data uploaded manually and not instantly actionable.[110] Additionally, issues with both fusing and sharing data streams remain a key problem, resulting in a lack of coordination and mismatches between higher-lever strategic situational awareness and tactical-unit situational awareness.[111] In a sense, force modernisation through systems like GIS Arta or DELTA has increased situational awareness and modernised artillery targeting, but has not unilaterally lifted the fog of war, decreased the chaos when contact with the enemy is made, nor negated the advantage of overwhelming numerical superiority.[112] Just as for drones, for its second counter-offensive Ukraine needed more tanks, armoured vehicles, personnel, mine-clearing equipment, and time to train its personnel, not more AI.

C. Cyberspace

The role that cyberspace plays – and will continue to play – in the future of warfare is a hotly disputed subject. Leading up to the February 2022 invasion, experts posited that a full-scale military operation by Russia – a state known for its offensive cyber operations – would be conducted in tandem with sophisticated and devastating cyberattacks on critical infrastructure and military and civilian targets.[113] So far, this has not materialised. While there has been noticeable uptick in cyberattacks targeting Ukraine, with a few high-profile ones, they have fallen short of the catastrophic pre-war predictions.[114] The large majority of attacks have been distributed denial of service attacks (DDoS) aimed at denying access to government (and other) websites, as well as "hack-and-leak" attacks aimed at stealing and leaking data for political purposes.[115] While the focus naturally is on Russian cyber operations, it must be noted that reported cyberattacks are distributed between both Russia and Ukraine, with around 331 attacks against Russia and 636 against Ukraine as of December 2023.[116]

Focusing first on Russia, it is difficult to authoritatively ascertain the reasons behind the relatively small impact of the country's cyber activity on battlefield outcomes. However, experts have pointed to several potential explanations. Firstly, the quality of Ukrainian defences is likely a factor. After years of experience with Russian cyber interference and close partnership with the United States on this front, Ukraine has built up strong cyber defences.[117] Additionally, extremely devastating Russian attacks such as the 2017 NotPetya attack, which resulted in over US$ 10 billion worth of damage, infecting and shutting down computers across the globe, as well as recurrent Ukrainian blackouts resulting from cyberattacks, offered a view of the devastating potential effects of such attacks.[118] This potentially led to an overestimation of the place that cyber activity might play as part of a Russian invasion and resulted in a better prepared Ukrainian side.

Secondly, expecting a quick victory, Russia's poor planning might have extended to the cyber domain. Expecting weak Ukrainian defences in cyberspace, Russia might have not invested substantial efforts into planning sophisticated cyberattacks and failed to integrate them into its overall plan for the invasion.[119] It is worth noting that successful offensive cyber operations require a great deal of planning, and successfully infiltrating an adversary's systems can take many months. For example, Russia's successful 2015 and 2016 attacks on the Ukrainian power grid took 19 months and two-and-a-half years of planning respectively. Therefore, successful offensive cyber operations are a planning- and intelligence-heavy activity and are only most effective when integrated with other weapons and consistent with a wider offensive. Additionally, they have to be tailored to specific targets, which reduces they flexibility. Alone and used ad hoc, cyberattacks lack the weight to have strategic military effects and compel an enemy to accept defeat.

In the rapidly shifting operational environment of the Ukrainian battlefield, Russia has resorted to fringe attacks on routers, firewalls and email servers.[120] Hence, Russian cyberattacks used in this way in Ukraine have been an annoyance at best, periodically creating confusion and inefficiencies, but doing little to advance Russia's military aims. Additionally, it is also difficult to "quantify" the impact of a cyberattack, assess the damage and decide that it has been a worthwhile, successful operation, which limits their usefulness in large-scale military offensive operations.[121]

Potentially, US diplomatic and deterrence efforts in cyberspace targeting Russia have also borne fruit and helped prevent catastrophic attacks on critical infrastructure, especially outside Ukrainian territory.[122] Moreover, while cyber attacks' relationship to conflict escalation is not clear, Russia might have restrained itself because of the potential for a catastrophic attack to escalate the conflict beyond what is intended, for example due to the possible cascading effects of cyberattacks on NATO allies.[123]

Private sector actors have also taken centre stage in Ukraine's cyber defence. Microsoft, for example, is credited with repelling Russian cyberattacks in the early stages of the invasion.[124] Similarly, Starlink detected a cyberattack on its satellites and installed the necessary patches on its systems – thus providing Ukraine with continued connection – with a speed that impressed even the Pentagon.[125] The Ukrainian authorities have been able to rely on a rich network of government and private sector actors, both foreign and domestic, to quickly identify and respond to cyber threats.[126]

As mentioned, Ukraine has not only been the victim, but also the perpetrator of offensive cyber activity during the conflict. Perhaps of greater interest to the study of the future of war than the use and impact – even if limited – of cyberattacks in the Ukrainian conflict is the case of the so called "IT Army of Ukraine", as a remarkable example of the growing use of surrogates by state and non-state actors in contemporary conflicts.[127] Indeed, the early days of the conflict saw the Ukrainian minister for digital transformation, Mykhailo Fedorov – prompted by tech entrepreneur Yegor Aushev – found the IT Army of Ukraine by calling on all hackers, hobbyists and cyber security professionals to conduct cyberattacks on Russian targets. This resulted in the creation of a Telegram channel with up to 300,000 users – along with smaller sub-channels – where targets are posted and operations "coordinated".[128] The actual number of active members helping the Ukrainian authorities is likely far below the number of users on the Telegram channel, but remains undisclosed.

According to research by the ETHZ Centre for Security Studies, the IT Army has a highly coordinated structure and activities, with a "core team" housed by Ukrainian authorities. While a central coordinating body does exist, the IT Army maintains a decentralised and diffuse organisational structure. Nonetheless, it is the "main hub for Ukraine's 'offensive' response in cyberspace in reaction to the Russian invasion".[129] Operations conducted by the IT Army have, for example, been the defacing of the Gazprom website and the website of the Russian internet service provider serving the Crimean Peninsula, and DDoS attacks on Russian rail- and flight-booking services.[130]

Other hacking collectives and groups that are not "officially" part of the IT Army of Ukraine are also in contact with the latter, and seem to help it with attacks. Irrespective of its real-world effectiveness, the IT Army is a perfect example of surrogacy: the act of offloading some of the burdens of warfighting onto others (individuals, non-state actors, and, increasingly, technologies themselves).[131] Surrogacy, however, entails some degree of loss of control, especially over escalation dynamics. As Krieg and Rickli argue, the desire of a patron to create a degree of dissociation from the surrogate's action – for plausible deniability and discretion – inevitably leads to a loss of direct control over the surrogate.[132] For instance, the involvement of the hacker group Anonymous early in the conflict raised fears that its actions could contribute to unwanted escalations.[133]

Ukraine is not alone in the use of surrogates in cyberspace. Russian international hacking activity is often attributed to shadowy Kremlin-backed groups such as "FancyBear", which hacked the US Democratic National Committee servers in 2016, or the "Sandworm" group responsible for the global NotPetya attack that originally targeted Ukraine in 2017. [134] The proliferation of non-state hackers even led the International Committee of the Red Cross to issue eight rules for "civilian hackers" during war and four obligations for states to restrain them.[135]

The use of the IT Army and extra-territorial hackers has also helped "spread" the front lines of the battlefield to outside Ukraine, blurring legal and normative lines. For example, if a Ukrainian citizen (or other national) conducts a cyberattack disrupting Russian troop communications or infrastructure, or in any way affects or reduces – even marginally – Russia's combat capabilities, should they be considered a legitimate target, even in a foreign country?[136]

All in all, evidence from the conflict shows that we must be more cautious and conservative over our predictions regarding the disruptive impact of cyberattacks in future conflicts. The assumption that a warring party will make use of devastating cyber tools and achieve tangible effects has not been entirely substantiated by the war in Ukraine. While the cyber domain remains an integral dimension of modern warfare, cyber tools have not shown dramatic kinetic impact and are not a silver bullet. Some experts therefore now argue that they are indeed not very effective at coercive and destructive action.[137]

Instead, it would be better to understand cyber operations as low-intensity disruption tools and tools of *subversion*. Utilised as such, cyber operations can contribute to weakening an adversary's defences and crucial infrastructure and undermining the legitimacy and efficacy of government institutions. For offensive cyber operations, this requires infiltrating the enemy's systems well before the beginning of hostilities. Thus, one could argue that cyber operations can be more active in "pre-war phases", to gather intelligence and understand the enemy's systems in order to identify vulnerabilities and exploit them later.

D. Information war

In a globalised conflict, especially one often framed as pitting competing world views against each other, promoting one's own narrative globally has become a necessity. Today's globalised information ecosystem therefore plays a crucial role in any conflict.[138] Part of Ukraine's "success" in slowing down Russia's early advance was its ability to muster international – mainly Western – public opinion to its side. President Zelensky capitalised on the narrative that depicts this conflict as the fight between democracy and autocracy, and made it politically costly for Western leaders to adopt any other political line than full support for Ukraine's war effort.[139] While this is not the only reason why Western governments are aiding Ukraine's war efforts, Ukraine's success in the information space has contributed to these governments' decisions to support Ukraine financially and militarily with arms transfers, a vital lifeline for Ukraine.[140] Winning Western public opinion has also been instrumental in mustering support for the sanctions regime aimed at stifling Russia's economy to adversely affect its war effort.

Actively engaging in the information domain has therefore not only contributed to securing the West's "narrative support" for Ukraine, but also actively impacted realities on the ground. Early in the war, Ukraine's – and particularly President Zelensky's – knack for social media communication relative to the Kremlin's was instrumental in achieving this.[141] Ukraine has also done this through a concerted, state-sponsored effort. A group of approximately 1,300 "software engineers, marketing managers, graphic designers and online ad buyers" called StandForUkraine was tasked with mobilising the support of the international community against Russia and spreading Ukrainian war propaganda across Western outlets and social media platforms.[142] The importance for the war of narratives in contributing to the support of a military cause is very visible now that "Ukraine fatigue" has set in among Western populations and leading Western governments, especially the United States, causing them to wind down their military support for Kyiv.[143]

The Kremlin also uses disinformation and propaganda as a tool of war both domestically and within its sphere of influence, as well as well as against its adversaries. Using its usual playbook, Russia has spread disinformation, notably through troll farms and bot accounts, to spread its narrative of the war.[144] For instance, the state agency tasked with protecting France against foreign digital interference, Viginum, recently published a report about a Russian disinformation network dubbed "Portal Kombat" comprising at least 193 sites.[145] The network aimed to present Russia's "special military operation" positively, denigrate Ukraine and its leaders in Western countries, and push potentially divisive and polarising narratives in Western societies. At home, the Kremlin exerts strict control over the Russian information ecosystem, harshly stifling dissent and passing new legislation effectively criminalising critique of the war.[146] It is reported that in 2022 the Kremlin spent US$ 1.9 billion on its domestic propaganda.[147] In occupied Ukrainian territories it is rerouting internet networks to Russia to better control the information space.[148]

While many commentators have claimed Ukraine's unilateral victory on the "information war" early in the conflict, this analysis is too narrow and Western-centric. While it is true that Ukraine managed to gain Western public opinion support very effectively at the beginning of the conflict and that, conversely, Russian disinformation efforts were less effective than in other instances such as during COVID-19 or the 2016 US elections, in other parts of the world Russia's information efforts were nonetheless very effective.[149]

Russian war narratives hit their target in places like China, India, Pakistan, Iran or South Africa, where genuine antipathy towards the West creates sympathy for Russia's cause. Here, Moscow sought to paint rising prices and shortages of food and gas as a consequence of Western actions.[150] The outcomes of the votes on the UN resolutions condemning Russia's invasion of Ukraine and expelling it from the Human Rights Council show that about half of the world's governments aligned with Russia or at least did not condemn Moscow's actions.[151] This was further aggravated by the escalation of the Israeli-Palestinian conflict, through which Russia was able to instrumentalise the inconsistencies felt by much of the world regarding the West's reaction to the conflict.[152]

While information warfare is nothing new, the tools that are now at a nation's disposal are, and both Ukraine and Russia have made successful use of them. Social media has been an important facet of the war, making it the first viral interstate war, and a key battleground on which the information war is fought at never-before-seen scale, affecting how "war is chronicled, experienced and understood".[153] Commercial satellite images have circulated information about troop movements, while smart phones have led to a proliferation of direct live-feed videos from the front lines.[154]

The increasing sophistication of AI-powered social-media algorithms that enable and dictate the diffusion of information online has been instrumentalised both by Ukraine and Russia. For example, in the first week of the war, videos on TikTok with the hashtags #Ukraine and #Russia garnered over 40 billion views.[155] This trend indicates that social media will increasingly become the primary distribution channel through which to wage information warfare. It must be noted that this trend started around 2014, with Islamic State's use of social media to garner support for its caliphate.[156] The "gaming" of these algorithmic dynamics has since become a key requirement of information warfare in order to spread narratives of the war, with the help of bots, trolls, and volunteers flooding social media channels with content, amplifying the reach and breadth of disinformation campaigns. Warring parties can today achieve both "granularity" by targeting people most susceptible to be impacted by information and scale as information spread globally through the internet.

E. Traditional armaments, tactics and personnel

For all the talk of the futuristic battlefields of the 21st century, Ukraine's battlefields share a great deal with the wars of the past. By and large, the conflict has been characterised by some age-old aspects of warfare. Planning failures, complex logistics, communication difficulties, personnel quality, organisational inefficiencies, the fog of war, declining morale, and substantial material and human losses can be all be found in the war in Ukraine. It is therefore useful to analyse some of these elements both to show their still-large influence in determining the direction of the conflict and their important role in determining the impact of the some of the above-mentioned emerging technologies.

Innovation and planning

Technology on its own cannot win a war. It must be integrated into a body of doctrines and operational concepts that allow it to be used to maximum effect. Russia's failures during the war's first year or Ukraine's failed second counter-offensive demonstrate how technology must be integrated with tactical innovations.

Russian planning failures seem to have stemmed from a combination of confirmation bias exacerbated by the small group of people familiar with the plans who relied on several false assumptions, lack of "red teaming", the failure to envision alternatives should the plan fail, and a subsequent incapacity to develop a revised course of action[157] Russia vastly under-estimated Ukrainian defences and capabilities, force mobilisation ability, and the population's will to resist.[158] Russia sent 200,000 troops across the border for a country-wide operation along four axes and expected to achieve victory in *ten days*.[159] To maintain operational surprise and secrecy, orders were only distributed 24 hours before the assault, which resulted in troops' lacking the tactical and operational contexts for their operations. In turn, this led to a lack of ammunition, fuel, food, maps and properly established communications.[160]

It was obvious early on that Russia struggled with combined arms operations, failing notably to support its armoured divisions with infantry, resulting in high casualty rates among mechanised units of tanks and armoured vehicles that were left completely exposed to Ukrainian troops equipped with anti-tank weaponry.[161] Lack of appropriate air defences and EW countermeasures also left columns of armoured vehicles vulnerable to Ukraine's drones. Operating under the assumption that they would not encounter heavy fighting, Russian troops behaved and moved around the battlefield (such as in long files on main highways) in ways that Ukrainian forces exploited to inflict disproportionate damage. Russia's failure to properly plan for and maintain complex logistics presented Ukraine with a key vulnerability to exploit. Ukraine used mobility and quickly deployable drones to strike the over-stretched Russian supply lines.

In essence, these failures created the conditions for Ukraine's mix of technology, innovation and tactics to be most effective. In later stages of the conflict, although Russia adapted many of its tactics, drone surveillance and AI-enabled targeting and strikes did not replace older, more brutal tactics. For example, Russia repeatedly resorted to "meatgrinder offensives" using disposable infantry units, often formed from ex-convicts and Wagner PMC personnel, in suicidal charges whose sole role was (and still is) to draw fire and reveal Ukrainian positions for targeting.[162]

In contrast, as seen with the relative failure of Ukraine's second counter-offensive in the fifth phase of the war, no matter the technological and tactical ingenuity of Ukraine's armed forces, dug-in and better prepared, trained and equipped Russian forces, which had adapted to the realities of the conflict, negated the power of asymmetric advantages gained though cheaper technological means. In preparation for Ukraine's second counter-offensive, and while Wagner forces pinned Ukraine in Bakhmut, Russian forces built the "Surovikin line" – named after the former commander of the Russian forces in Ukraine, Sergey Surovikin – a 130 km defensive line comprising fortifications, trench networks, armoured vehicle traps such as "dragon's teeth", expansive mine fields, and positions manned by experienced troops. In stark contrast to their first offensive, Ukraine lost up to 20% of all material committed in the first two weeks of its second offensive, most of it Western equipment the country had spent the previous year lobbying for.[163] In this context, Ukraine quickly abandoned its Western-style combined arms manoeuvre operation and returned to its earlier tactics, prioritising operations through small infantry units.[164] While proving less deadly for Ukrainian forces, these tactics have also been much slower, and have failed to produce the desired breakthrough.

In this changed tactical environment, where Russia has understood, adapted and largely caught up technologically, Ukraine's early innovation and technology-enabled advantages have now largely ended, with Russia gradually closing both gaps with Ukraine, and Ukraine's lead in innovation failing to translate into battlefield results beyond the tactical level.

Traditional armaments, and quantity and quality of personnel

As of March 2024, Russia has suffered an estimated 200,000-300,000 casualties and has lost around 14,000 pieces of equipment.[165] While a more closely guarded secret, Ukraine's loses are similarly staggering, with an estimated 130,000 casualties and over 5,000 pieces of equipment lost.[166] As the war becomes more protracted and both sides dig themselves in, the conflict's similarity with those of the 20th century has come into sharper focus. The conditions imposed by such attrition has highlighted the importance of stocks of ammunition, the quantity and quality of personnel, and the sheer quantities of traditional armaments still needed for a successful campaign.

The use of artillery has perhaps been the most pervasive feature of the conflict, demonstrating that it remains an important aspect of modern warfare. At the peak of its offensive campaign Russia was firing upwards of 60,000 shells a day, with Ukraine firing at most around 7,000 shells daily.[167] In 2022 it is estimated that Russia fired upwards of 10 to 11 million artillery shells.[168]

These rates of fire have meant that Ukraine's partners, on whom the country is now entirely reliant for armaments, have struggled to meet demand. Whereas the European Union (EU) promised approximately 1 million rounds in the next year in the spring of 2023, by December 2023 only 300,000 shells were delivered.[169] To sustain Ukraine's desired rate of fire, it would need to receive over 350,000 shells per month, or over 4 million per year.[170] On top of that, it would need over 1,800 replacement barrels for artillery pieces per year.[171] However, in February 2023 EU production only stood at around 300,000-400,000 shells annually.[172]

In January 2024 Avdiivka was the first Ukrainian city to fall since Bakhmut in May 2023. This is in large part due to Ukraine's critical lack of ammunition, resulting in the need to utilise it sparingly.[173] With a quantitative disadvantage of five to one, Ukrainian soldiers have had to ignore small groups of Russian soldiers and fire only at larger groups.[174]

Additionally, even the prevalence of novel strike capabilities such as drones has further entrenched, not reduced or replaced, the importance of heavy artillery.[175] As previously mentioned, drones' relative limitation in payload and ability to concentrate large amounts of firepower has served as a reminder of the necessity of heavy artillery.[176] In this setting, the impact of drones has been the greatest in enhancing, not replacing, artillery, making it more accurate, quicker firing and more efficient. However, Ukraine's efforts to produce over 100,000 drones a month are likely still motivated by a desire to make up for deficiencies in artillery, which has notably worried observers.[177]

The centrality of artillery – responsible for over 70% of all casualties in the war – has put pressure on the EU, United States and NATO to replenish their stocks and ramp up their production.[178] Struggling to keep up with its own depleting stocks, Russia has, for example, had to turn to North Korea for shells.[179] More modern and more feared ordnance such as hypersonic missiles have had comparatively little impact on the conflict besides their initial "shock effect". While the war marks their first operational use, their presence has been more symbolic than useful for Russia. Representing some of the most modern weaponry in the Russian arsenal, hypersonic missiles have been used sparingly compared to other alternatives such as traditional ballistic missiles and Iranian Shahed 136 drones. This points to the fact that much of their more destabilising and disruptive effects and some of their capabilities may have been exaggerated.[180]

After artillery, tanks and armoured vehicles remain the most important assets in both Ukraine's and Russia's offensive and defensive operations.[181] As evidenced by Ukraine's lobbying efforts throughout 2023, it is tanks and armoured vehicles, besides ammunition, on which it focused. While enhanced – as well as impeded – by the pervasive usage of UAVs, Ukraine's assaults remain spearheaded by mine-clearing equipment, tanks, and armoured vehicles, which are themselves often destroyed by enemy mines, tanks, and artillery.[182]

The failure of the Ukrainian counter-offensive is also not the death knell of the tank versus cheaper alternatives such as drone. In fact, the vulnerability of armoured vehicles and tanks cannot be wholly attributed to drones alone.

Each side's inability to establish air superiority and the resulting need to mount offensives without traditional close air support has vastly increased their vulnerability and exacerbated the impact of drones. Focusing on numbers only, such as the number of tanks lost by each side, is a poor indication of their performance and importance, which are the result of a complex interaction of many parameters specific to their operational environment and use.[183] Therefore, their use and performance in unfavourable conditions (in this case positional warfare and the difficulty of conducting combined arms operations) should not be the basis to declare any weapons system obsolete.[184] These armaments remain by far the most important aspect of this conflict, and crucial systems in future warfare.

Furthermore, the quality and quantity of personnel have been a red thread throughout the conflict, emphasising that manpower remains a determining factor of success in modern warfare. As one expert notes, "the Ukraine War demonstrates the primacy of competence over technology".[185] Personnel quality, for example, played a key role in both the success and failure of Ukraine's two counter-offensives, respectively. Russia's poor preparation and the dismal state of its troops occupying Ukraine's north due to poor military leadership were key contributors to the success of Ukraine's first counter-offensive.[186] With Russia having moved much of its most experienced units south to counter Ukraine's southern thrust and lacking the necessary manpower to man the almost 1,600 km front, territory fell at a rapid rate, with Russian troops lacking the direction, motivation, and capability to fight back.[187] The war's previous phase had sufficiently degraded Russian forces, which were operating at 25% capacity in some areas, enabling Ukraine's mix of technology and tactics to have the greatest effect.[188]

Furthermore, the quality of personnel permeates through to the use of drones, and is one of the most important factors in determining how impactful the use of drones is.[189] Depending on the quality of the pilot, the success rate of an FPV drone flight can vary from 10% to 80%.[190] While Russia is slowly catching up, in this field Ukraine has a crucial advantage, gained through its concerted national efforts to produce high-quality pilots.[191]

When facing Russian troops in their 2023 offensive, it was the lack of experience and training of Ukraine's newly formed brigades that showed and contributed to the failure of the operation. Ukraine's units reportedly made mistakes in planning, coordinating artillery fire, operating equipment and orientating at night.[192] Ukrainian planners diluted their forces by focusing on three axes, while their US allies urged them to focus on one axis towards Melitopol.[193] This dilution magnified the essential role played by units and the ability to sustain a war of attrition. In terms of units, forces on both sides had few opportunities to train at scale, and it is precisely this lack of training and time to prepare that has been identified as the foremost reason for the 2023 offensive's failure.[194] Most troops had never seen combat before, had been given five weeks of training, most of which did not focus on complex offensive operations, and had barely the knowledge needed to operate their new Western equipment.[195] For success, not only was more equipment needed, but also more time to train personnel. With heavy attrition rates, a dwindling pool of potential recruits and compressed time scales, these will be increasingly difficult to achieve, thereby degrading both nations' combat power. As Watling notes, "the heavy attrition of experienced junior officers and trained field-grade staff has limited the scale at which offensive action can be synchronised".[196]

As the war stretches into its third year, new rounds of mobilisation are becoming a requirement for both nations.[197] With casualty rates between 200 and 900 per day, the capacity to mobilise, train, and deploy combat-capable troops and renew materials and ammunition will play the central role in determining the direction of the conflict and the outcome of both offensive and defensive operations.

V. What can we learn from this?

Careful analysis of the events of the various phases of the conflict point to a key lesson: while the character of warfare is changing, it is doing so at a relatively slow pace. Indeed, although new technologies and innovations have made their way onto the battlefields of Ukraine, the conflict remains defined by some age-old characteristics of warfare. It therefore tells us that our approach to studying the future of warfare should be measured and conservative, and not based on predictions of vast, rapid, and dramatic changes brought about by technological disruption.

Firstly, drones are increasingly a key feature of conflicts, with some transformative effects. Their high-profile use in Ukraine and the vulnerability of mechanised units and infantry to drone attacks are likely to spur the further proliferation of these capabilities among the world's militaries.[198] At present, drones are enhancing the lethality of modern battlefields and will likely drive a shift in how large-scale offensive operations are conducted in the future.[199] Furthermore, the largely commercial and cheap nature of these drones effectively accelerates the trend of sourcing civilian technology for military repurposing and making them a quintessentially dual-use technology. This, coupled with the enlisting of civilian drone hobbyists as operators and "modificators" of drones, increases the importance of both civilians and commercial companies in the future of drone warfare.

The proliferation of drone usage in conflict will converge with the increasing trend of the autonomy of weapons systems. This will lead to an increased presence of systems with a growing array of autonomous functions on future battlefields. As seen by the difficulties encountered by efforts focused on the international regulation of autonomous weapons systems (through, for instance, the UN Governmental Group of Experts in the Area of Lethal Autonomous Weapons Systems), the trends towards embedding autonomy in a wider array of weapons systems and functions and deploying increasingly autonomous weapons systems is very likely to continue. Both Ukraine and Russia already claim to be fielding autonomous capabilities. This indicates that in high-intensity conflicts the immediate pressures of the battlefield are stronger than the normative and ethical pressures currently holding autonomous weapons systems in check. Should both Russia and Ukraine continue to increase the autonomy of their weapons systems, with tangible "positive" results and without international regulation, efforts towards the development and deployment of these capabilities worldwide would greatly accelerate.

However, as previously shown, drones have proven not to be silver bullet. While their presence has been transformational, some of their early impact was a function of Russian failures, inefficiencies and strategy as much as the technology itself. As exemplified by the current needs of both armed forces, drones have not reduced the importance of legacy systems such as artillery, armoured vehicles and tanks. As Borsari and Davis aptly note, drones cannot achieve the ultimate goal of war: they cannot seize and hold terrain.[200] While drones have contributed to "freezing" the front line, offsetting Russia's advantages in this war, Ukraine requires more expensive and advanced armaments – and in great quantities – not only cheaper technological alternatives.[201] Some experts, therefore, have held that evidence from recent conflicts does not point to a so-called "drone revolution" in warfare.[202] They further note that drones have not eliminated close combat, and that they can only be effective if they are operated by skilled military personnel and integrated with other multilayered and conventional systems, once again underlying the importance of doctrinal innovation.[203]

While these points are relevant, more recent analyses of the use of drones in Ukraine shows that a drone revolution is indeed under way, just perhaps not of the kind scholars had anticipated. The advantage lies in their small size, numbers, low flight profile and low cost.[204] However, it must be noted that the current cost-effectiveness of drone usage might not remain true for ever. Russia is already innovating and investing significantly in drone countermeasures and EW capabilities. This will inevitably require drones to be fitted with more advanced electronics to evade ever more effective countermeasures. This measure/countermeasure dynamic is likely to drive up the cost of drones,[205] which in turn is also likely to further drive increases in drone autonomy to effectively operate in communication-deprived environments.[206] This will eventually reinforce the already emerging desire to operate autonomous drone swarms on the battlefield and likely act as a further driver of their eventual development, deployment, and proliferation.

Asymmetric tactics and capabilities in conflict, especially as implemented by cheap technological alternatives, have therefore shown both their successes and limitations. An important takeaway is that quantities of traditional equipment still matter, and disinvesting from traditional aspects of defence, such as tanks and heavy artillery, is dangerous. When restraints are removed in high-intensity conflicts – especially attritional conflicts – stocks of ammunition, personnel and traditional weapons systems remain foundational for victory. Digital means to wage war, such as cyberattacks, are now part of modern warfighting and will continue to be so. However, their coercive power remains limited, as there is little evidence to support their ability to achieve tangible, measurable operational effects (especially kinetic effects) to advance military objectives. They are perhaps better understood as tools of subversion. As Robinson states, in Ukraine "new technologies are being used to supplement and reinforce existing ways of waging war, rather than change them".[207] Yet in light of recent disruptive developments in AI, such as generative AI and neurotechnologies with emerging brain-computer interfaces, it is very likely that subversion will increasingly become a tool of modern warfare.[208]

The age of industrial warfare is not yet behind us, and a solid industrial base remains a key element of victory in 21st century warfare.[209] The traditional principles of warfare remain vital elements of military victory. The quality of personnel; the relevance of doctrinal thinking; the quality of plans; the importance of morale, motivation, deception, and strategic and tactical surprise; the complexity of logistics; and, of course, the fog of war will endure.

Other emerging technologies and innovations, such as various AI-enabled applications, have made sporadic appearances throughout the conflict, but have been of limited impact so far. Here, two similar observations can be made.

Firstly, their very presence is a testament to their military potential and the willingness of armed forces to make use of them. AI and other emerging technologies, sometimes cheaply and commercially available, are and will be militarised.[210] Warring parties have shown their appetite to use Deepfakes, NLP algorithms and AI-enabled automation of disinformation in conflict. As an analytical enabler, AI-enabled data collection, analysis and the networking of various information streams will continue to grow in importance. The ability to have an AI-generated operational picture of the battlefield has been instrumental in helping Ukraine make more efficient use of its lesser resources. AI will surely therefore continue to make inroads in the military domain.[211]

Secondly, however, the conflict is also emphasising that emerging technologies – for now – still have limited effects and importance in determining a war's outcome. Emerging technologies will continue their slow and incremental adoption alongside traditional armaments, which still dominate the battlefield.[212] What we are witnessing is the very beginning of a trend that will continue and likely increase in the future. For now, however, in most cases emerging technologies' integration into high-intensity conflict remains marginal. Yet the fact that most, if not all, of these technologies come from the commercial sector means that a country's technology ecosystem and its successful leveraging for military ends will be key to 21st century warfare. In this respect, Ukraine will continue to act as a test bed for many AI-driven military technology innovations, while developments in science and technology will continue as important drivers of global power dynamics.

All in all, the role of emerging technologies cannot be taken out of their context and operational environment at the time of their use. Lessons should not be drawn only from either the technologies themselves or their presence alone, with no consideration for the conditions that allowed their use to maximum effects. Determining the role these technologies will have in future wars, especially gauging their role in determining battlefield outcomes, is therefore not simply a question of which technologies do and will exist, but a function of a more complex mix of factors, including their integration into battlefield tactics, operational environment conditions or the enemy's strategy.[213] Many of the advantages gained through cheaper technological alternatives in Ukraine were gained in "permissive" environments. Current battlefield realities show that a technological advantage is temporary, and only lasts for as long as the enemy has not adapted to it.[214] Therefore, perhaps more important than the technologies themselves is the imperative to adapt, where success lies in the ability to integrate new systems and technologies into operations and tactics and exploit the often-momentary advantage they confer.[215] In an era of exponential technological developments,[216] the pace of adoption and adaptation will only accelerate and require militaries to be ever more agile and reactive.

VI. Conclusion

As one of the most important conflicts since the end of the Cold War, the war in Ukraine can provide us with a contemporary example of how the character of warfare is changing. It can help us understand the extent to which emerging technologies have permeated the military domain and help us gauge their impact. All in all, the war has come to confirm many of the trends in the modernisation of the battlefield, while showing that even as new technologies come to alter the battlefield by introducing new means of warfare and new actors and complexifying the conduct of hostilities, many aspects of the conduct of warfare remain the same.

Ukraine is best understood as a testing ground for the use of emerging technologies in war, ushering in a period where the old and the new start to coexist. Emerging technologies have conferred asymmetric advantages, introduced more actors to hostilities, and provided cheaper alternatives to achieving battlefield effects. Drones have become a pervasive feature of this conflict, offering unprecedented battlefield situational awareness and a cheap, off-the-shelf strike capability. Because of them, there is nowhere to hide on 21st century battlefields, increasing their lethality. AI has proven that is has begun to make inroads in the military domain, acting as an analytical enabler, force multiplier and disruptor, showing that predictions of the militarisation of AI are well founded and are likely to increasingly define future battlefields.[217]

However, many of the advantages gained through these emerging technologies were gained in permissive environments and exacerbated by faulty tactics, organisational dysfunction or poor personnel quality. Their impact, therefore, cannot be wholly attributed to the characteristics of the technologies themselves, but how and when they were used (i.e. under which conditions), and needs to be understood as part of its broader context. In non-permissive environments, their impact has been much more muted. Technology and innovation have often stumbled in the face of an overwhelming quantity of traditional armaments and well-executed tactics.

Even as emerging technologies have provided new ways and methods of fighting, the conduct of the Ukraine war remains for now largely defined by legacy systems such as tanks, artillery, and armoured vehicles. Technology has done little to lift the fog of war and has not reduced the importance of the sheer quantity of armaments and ammunition needed in modern conflicts, as well as the quantity and quality of personnel. Analysis and predictions regarding the place of emerging technologies in the future of warfare should not forget that in essence warfare is a human affair. Hence, adopting a technology-centric view of it that perhaps over-emphasises the results of the technology bonanza of the 21st century is giving a skewed version of what war might look like in the future.

The present conflict should serve as a reminder that war's enduring nature has a bearing on its character. As a contest of wills in which humans inflict violence on each other, the place that technology takes in warfare can only grow so much. Ukraine's battlefields show that even as war is undoubtedly changing, it's future will still share much with its past.

Endnotes

1 T.K. Adams, "Future Warfare and the Decline of Human Decision-making", *Parameters*, Vol.41(4), 2011, https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=2600&context=parameters.

2 M. Raska, "The Sixth RMA Wave: Disruption in Military Affairs?", *Journal of Security Studies*, Vol.44(4), 2021, https://doi.org/10.1080/01402390.2020.1848818.

3 D. Rotolo et al., "What Is an Emerging Technology?", *Research Policy*, Vol.44(10), 2015, pp.1827-1843, https://doi.org/10.1016/j.respol.2015.06.006.

4 A. Krieg and J.-M. Rickli, *Surrogate Warfare: The Transformation of War in the 21st Century*, Georgetown University Press, 2019.

5 Adams, 2011.

6 J. Stone, "Cyber War Will Take Place!", *Journal of Strategic Studies*, Vol.36(1), 2013, pp.101-106, http://dx.doi.org/10.1080/01402390.2012.730485; T. Rid, "Cyber War Will Not Take Place", *Journal of Strategic Studies*, Vol.35(1), 2012, pp.5-32, https://doi.org/10.1080/01402390.2011.608939.

7 S. Biddle, "The Past as Prologue: Assessing Theories of Future Warfare", *Security Studies*, Vol.8(1), 1998, pp.1-74, https://doi.org/10.1080/09636419808429365.

8 A.F. Krepinevich, *The Origins of Victory: How Disruptive Military Innovation Determines the Fates of Great Powers*, Yale University Press, 2023.

9 M. Raska and R.A. Bitzinger (eds), *The AI Wave in Defence Innovation: Assessing Military Artificial Intelligence Strategies, Capabilities and Trajectories*, Routledge, 2023, https://www.routledge.com/The- AI-Wave-in-Defence-Innovation-Assessing-Military-Artificial-Intelligence/Raska-Bitzinger/p/book/9781032110752.

10 Ibid.

11 J.-M. Rickli and F. Mantellassi, "Artificial Intelligence in Warfare: Military Uses of AI and Their International Security Implications", in Raska and Bitzinger (eds), 2023.

12 Ibid.

13 Ibid.

14 Some countries at the United Nations Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems (GGE on LAWS) maintain the position that autonomy in weapons systems could enhance both these systems' accuracy and commanders' situational awareness, thus assisting in IHL compliance and reducing civilian casualties. See, for example, "US Statement at the GGE on LAWS during the Discussion on Agenda Item 5(D) 2021", https://geneva.usmission.gov/2021/08/05/u-s-statement-at-the-gge-on-laws-during-the-discussion-of-agenda-item-5d/.

15 P. Robinson, "The Russia-Ukraine Conflict and the (Un)Changing Character of War", *Journal of Military and Strategic Studies*, Vol.22(2), 2022, https://jmss.org/article/view/76588/56337.

16 H. Cooper, "Heavy Losses Leave Russia Short of Its Goal, U.S. Officials Say", *New York Times*, 11 August 2022, https://www.nytimes.com/2022/08/11/us/politics/russian-casualties-ukraine.html.

17 M. Clark et al., "Russia-Ukraine Warning Update: Russian Offensive Campaign Assessment, February 27", Institute for the Study of War and AEI's Critical Threats Project, 27 February 2022, https://www.understandingwar.org/backgrounder/russia-ukraine-warning-update-russian-offensive-campaign-assessment-february-27.

18 M. Zabrodskyi et al., "Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine: February–July 2022", Royal United Services Institute (RUSI), 30 November 2022, https://static.rusi.org/359-SR-Ukraine-Preliminary-Lessons-Feb-July-2022-web-final.pdf.

19 BBC, "Ukrainian Casualties: Kyiv Losing up to 200 Troops a Day – Zelensky Aide", 9 June 2022, https://www.bbc.com/news/world-europe-61742736.

20 Cooper, 2022.

[21] F.W. Kagan et al., "Russian Offensive Campaign Assessment, April 5", Institute for the Study of War and AEI's Critical Threats Project, 5 April 2022, https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-april-5.

[22] J.-M. Rickli, "Invasion russe de l'Ukraine: des victoires tactiques mais un désastre stratégique", *Le Temps*, 26 May 2022, https://www.letemps.ch/opinions/invasion-russe-lukraine-victoires-tactiques-un-desastre-strategique.

[23] K. Lawlor et al., "Russian Offensive Campaign Assessment, September 20", Institute for the Study of War and AEI's Critical Threats Project, 20 September 2022, https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-september-20.

[24] BBC, "Ukraine War in Maps: Tracking the Russian Invasion", 13 September 2022, https://www.bbc.com/news/world-europe-60506682.

[25] *New York Times*, "Maps: Tracking the Russian Invasion of Ukraine", 9 June 2023, https://www.nytimes.com/interactive/2022/world/europe/ukraine-maps.html.

[26] M. Santora, "For Ukraine, Keeping the Lights on Is One of the Biggest Battles", *New York Times*, 17 November 2022, https://www.nytimes.com/2022/11/17/world/europe/ukraine-electricity-water-infrastructure.html.

[27] K. Stepanenko et al., "Russian Offensive Campaign Assessment, May 20, 2023", Institute for the Study of War and AEI's Critical Threats Project, 20 May 2023, https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-may-20-2023.

[28] S. Bell, "Ukraine War: The Battle of Bakhmut Is Not about Seizing Vital Ground – It Is about Maximising Enemy Casualties", Sky News, 13 May 2023, https://news.sky.com/story/ukraine-war-the-battle-of-bakhmut-is-not-about-seizing-vital-ground-it-is-about-maximising-enemy-casualties-12879310; J. Watling and N. Reynolds, "Meatgrinder: Russian Tactics in the Second Year of Its Invasion of Ukraine", RUSI, 19 May 2023, https://static.rusi.org/403-SR-Russian-Tactics-web-final.pdf.

[29] G. Gressel, "Beyond the Counter-offensive: Attrition, Stalemate and the Future of War in Ukraine", European Council on Foreign Relations, 18 January 2024, https://ecfr.eu/publication/beyond-the-counter-offensive-attrition-stalemate-and-the-future-of-the-war-in-ukraine/#the-persistence-of-attrition-warfare.

[30] N. Wolkov et al., "Russian Offensive Campaign Assessment, November 21, 2023", Institute for the Study of War and AEI's Critical Threats Project, 21 November 2023, https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-november-21-2023.

[31] M. Hernandez and J. Holder, "Defenses Carved into the Earth", *New York Times*, 14 December 2022, https://www.nytimes.com/interactive/2022/12/14/world/europe/russian-trench-fortifications-in-ukraine.html. It must be noted that while their US allies advised Ukraine to concentrate its forces along one axis, Ukrainian forces opted for a three-axes offensive instead. See *Washington Post*, "Miscalculations, Divisions Marked Offensive Planning by U.S., Ukraine", 4 December 2023, https://www.washingtonpost.com/world/2023/12/04/ukraine-counteroffensive-us-planning-russia-war/.

[32] Ibid.

[33] H. Mongillio, "A Brief Summary of the Battle of the Black Sea", US Naval Institute, 15 November 2023, https://news.usni.org/2023/11/15/a-brief-summary-of-the-battle-of-the-black-sea. The first attack on the Sevastopol headquarters was carried out using a small long-range drone, while the final strike was conducted by a Storm Shadow missile.

[34] V. Melkozerova, "Ukrainian Attacks Force Russia to Relocate Black Sea Fleet", *Politico*, 6 October 2023, https://www.politico.eu/article/ukraine-attack-crimea-russia-ships-relocate/.

[35] Gressel, 2024.

[36] C. Méheut and A.E. Kramer, "Ukraine's Top Commander Says War Has Hit a 'Stalemate'", *New York Times*, 2 November 2023, https://www.nytimes.com/2023/11/02/world/europe/ukraine-zaluzhny-war.html.

[37] For context, it is estimated that Russia has now lost more tanks than it started the war with – around 3,000.

[38] F. Farrell, Ukraine Struggles to Ramp up Mobilization as Russia's War Enters 3rd Year", *Kyiv Independent*, 23 January 2024, https://kyivindependent.com/move-to-expand-mobilization-brings-ukrainian-society-face-to-face-with-immense-pressure-of-war/.

39 K. Hird et al., "Russian Offensive Campaign Assessment, March 14, 2024", Institute for the Study of War and AEI's Critical Threats Project, 14 March 2024, https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-march-14-2024.

40 F. Borsari and G.B. Davis, *An Urgent Matter of Drones*, Center for European Policy Analysis, 27 September 2023, https://cepa.org/comprehensive-reports/an-urgent-matter-of-drones/; S. Pettyjohn, "Evolution Not Revolution: Drone Warfare in Russia's 2022 Invasion of Ukraine", Center for a New American Security, February 2024, https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/CNAS-Report-Defense-Ukraine-Drones-Final.pdf.

41 D. Sabbagh, "War-enabling, Not War-winning: How Are Drones Affecting the Ukraine War?", *The Guardian*, 15 May 2022, https://www.theguardian.com/world/2022/may/15/war-enabling-not-war-winning-how-are-drones-affecting-the-ukraine-war.

42 J. Arraf, "Crowdfunding a War: How Online Appeals Are Bringing Weapons to Ukraine", *New York Times*, 10 May 2022, https://www.nytimes.com/2022/05/10/world/middleeast/ukraine-crowdsourcing-online-donations.html; Vice, "Ukrainians Are Bombing Russians with Custom Drones", video, https://video.vice.com/en_us/video/ukrainians-are-bombing-russians-with-custom-drones/6267c399f85e1243221cd521.

43 Ibid.; Arraf, 2022.

44 D. Axe, "Explosive Drones Are Everywhere in Ukraine. So the Infantry Head Underground, and Erect Screens", Forbes, 16 November 2023, https://www.forbes.com/sites/davidaxe/2023/11/16/explosive-drones-are-everywhere-in-ukraine-so-the-infantry-head-underground-and-erect-screens/?sh=2310e5934b88.

45 I. Khurshudayan et al., "Russia and Ukraine Are Fighting the First Full-scale Drone War", *Washington Post*, 2 December 2022, https://www.washingtonpost.com/world/2022/12/02/drones-russia-ukraine-air-war/?utm_medium=social&utm_campaign=wp_main&utm_source=twitter.

46 M. Santora, "They Come in Waves: Ukraine Goes on Defense against a Relentless Foe", *New York Times*, 4 February 2024, https://www.nytimes.com/2024/02/04/world/europe/ukraine-defense-east.html.

47 J. Buckby, "Video Shows Ukrainian Troops Using a Chinese-made Drone to Watch Missiles Strikes on Russian Forces", *Business Insider*, 6 June 2022, https://www.businessinsider.com/ukrainians-use-chinese-dji-drones-to-watch-strikes-on-russians-2022-6?r=US&IR=T.

48 D. Kunertova, "Drones Have Boots: Learning from Russia's War in Ukraine", *Contemporary Security Policy*, 4 October 2023, https://doi.org/10.1080/13523260.2023.2262792.

49 D. Kunertova, "The Ukraine Drone Effect on European Militaries", *Policy Perspectives*, Vol.10(15), December 2022, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/PP10-15_2022-EN.pdf; Pettyjohn, 2024.

50 S. Skove, "Ukraine's Soldiers Use Cheap Tech to Hide from Russia's Deadly Drones", Defense One, 21 December 2023, https://www.defenseone.com/threats/2023/12/ukraines-soldiers-use-cheap-tech-hide-russias-deadly-drones/392957/.

51 Pettyjohn, 2024.

52 I. Pannell and A. Weintraub, "Inside Ukraine's Efforts to Bring an 'Army of Drones' to War against Russia", ABC News, 14 September 2023, https://abcnews.go.com/US/inside-ukraines-efforts-bring-army-drones-war-russia/story?id=103152130.

53 Borsari and Davis, 2023.

54 Gressel, 2024.

55 Reuters, "Ukraine to Produce One Million Drones Next Year, Zelenskiy Says", 19 December 2023, https://www.reuters.com/world/europe/ukraine-produce-one-million-drones-next-year-zelenskiy-says-2023-12-19/.

56 R. Amran, "Zelensky: Ukrainian Military to Create Separate Branch Dedicated to Drones", *Kyiv Independent*, 6 February 2024, https://kyivindependent.com/zelensky-to-create-separate-division-of-military-focused-on-drones/.

57 BBC, "Sea Drones: What Are They and How Much Do They Cost?", https://www.bbc.com/news/world-europe-66373052.

58 H.I. Sutton, "Suspected Ukrainian Explosive Sea Drone Made from Recreational Watercraft Parts,", USNI News, 11 October 2022, https://news.usni.org/2022/10/11/suspected-ukrainian-explosive-sea-drone-made-from-jet-ski-parts.

59 D. Axe, "The Russian Black Sea Fleet May Have Lost Another Flagship", 29 October 2022, https://www.forbes.com/sites/davidaxe/2022/10/29/the-russian-black-sea-fleet-may-have-lost-another-flagship/?sh=70b21fb592e6; M. Zafra and J. McClure, "Sea Drones and the Counteroffensive in Crimea", Reuters, 27 July 2023, https://www.reuters.com/graphics/UKRAINE-CRISIS/CRIMEA/gdvzwrmrlpw/.

60 M. Cancian, "Ukraine's Victory at Sea", *Foreign Affairs*, 8 February 2024, https://www.foreignaffairs.com/ukraine/ukraines-victory-sea.

61 S. Bendett, "The Ukraine War and Its Impact on Russian Development of Autonomous Weapons", Atlantic Council, 30 August 2022, https://www.atlanticcouncil.org/content-series/airpower-after-ukraine/the-ukraine-war-and-its-impact-on-russian-development-of-autonomous-weapons/.

62 S. Bendett, "Where Are Russia's Drones?", Defense One, 1 March 2022, https://www.defenseone.com/ideas/2022/03/where-are-russias-drones/362612/.

63 I. Facon, "Proliferated Drones: A Perspective on Russia", Center for a New American Security, 12 May 2016. https://www.frstrategie.org/sites/default/files/documents/publications/autres/2016/2016-facon-cnas-proliferated-drones.pdf; Bendett, 30 August 2022. However, it must be noted that as of early March 2024 successful Russian strikes in the Ukrainian rear areas on Patriot systems, HIMARS and groups of helicopters show an improvement in Russia's drone-enabled intelligence, surveillance, and reconnaisance capabilities and a shortening of the loop between target identification and engagement.

64 Bendett, 30 August 2022.

65 P. Luzin, "Russian Military Drones: Past, Present and Future of the UAV Industry", Foreign Policy Research Institute, November 2023, https://www.fpri.org/wp-content/uploads/2023/11/russian-military-drones-.pdf.

66 S.B. Freedberg, "How Not to Innovate: Russia Plays Catch-up to Ukraine on Drones", Breaking Defense, 30 May 2023, https://breakingdefense.com/2023/05/how-not-to-innovate-russia-plays-catch-up-to-ukraine-on-drones/.

67 S. Bendett and J.A. Edmonds, *Russia's Use of Uncrewed Systems in Ukraine*, Center for Naval Analyses, March 2023, https://www.cna.org/reports/2023/03/Russian-Uncrewed-Systems-Ukraine.pdf.

68 E. Schmidt, "Ukraine Is Losing the Drone War", *Foreign Affairs*, 22 January 2024, https://www.foreignaffairs.com/ukraine/ukraine-losing-drone-war-eric-schmidt.

69 Pettyjohn, 2024.

70 *The Economist*, "How Cheap Drones Are Transforming Warfare in Ukraine", 5 February 2024, https://www.economist.com/interactive/science-and-technology/2024/02/05/cheap-racing-drones-offer-precision-warfare-at-scale.

71 BBC, "Ukraine Conflict: How Are Drones Being Used?", 22 August 2022, https://www.bbc.com/news/world-62225830.

72 F. Bajak and O. Stashevskyi, "Deadly Secret: Electronic Warfare Shapes Russia-Ukraine War", AP News, 4 June 2022, https://apnews.com/article/russia-ukraine-kyiv-technology-90d760f01105b9aaf1886427dbfba917; A. Shoaib, "Ukraine's Drones Are Becoming Increasingly Ineffective as Russia Ramps up Its Electronic Warfare and Air Defences", *Business Insider*, 3 July 2022, https://www.businessinsider.com/drones-russia-ukraine-war-electronic-warfare-2022-7?r=US&IR=T.

73 Ibid.

74 Kunertova, 2022.

75 Zabrodskyi, 2022.

76 Watling and Reynolds, 19 May 2023.

77 The Brave1 accelerator is a Ukrainian incubator for defence technology, providing organisational, informational and financial support for defence technology projects in Ukraine. For more information, see https://brave1.gov.ua/en/.

78 I. Varenytsia, "Drones Are Hit and Miss for Ukrainian Soldiers", Reuters, 23 January 2024, https://www.reuters.com/world/europe/drones-are-hit-miss-ukrainian-soldiers-2024-01-23/.

79 Ibid.

80 *The Economist*, "Ukraine's Commander-in-chief on the Breakthrough He Needs to Beat Russia", 1 November 2023, https://www.economist.com/europe/2023/11/01/ukraines-commander-in-chief-on-the-breakthrough-he-needs-to-beat-russia.

81 J. Watling, "The War in Ukraine Is Not a Stalemate", *Foreign Affairs*, 3 January 2024, https://www.foreignaffairs.com/ukraine/war-ukraine-not-stalemate.

82 U. Franke and J. Soderstrom, "Star Tech Enterprise: Emerging Technologies in Russia's War on Ukraine", European Council on Foreign Relations, 5 September 2023, https://ecfr.eu/publication/star-tech-enterprise-emerging-technologies-in-russias-war-on-ukraine/.

83 Rickli and Mantellassi, 2023.

84 J.-M. Rickli et al., "Peace of Mind: Cognitive Warfare and the Governance of Subversion in the 21st Century", Geneva Centre for Security Policy, Policy Brief No. 9, August 2023, https://dam.gcsp.ch/files/misc/pb-9-rickli-mantellassi?.

85 The OODA process is the cornerstone of modern effect-based operations. For both a description and critique of the concept, see D.J. Briant, "Rethinking OODA: Toward a Modern Cognitive Framework of Command Decision Making", *Military Psychology*, Vol.18(3), 2006, pp.183-206, https://www.researchgate.net/profile/David-Bryant-7/publication/233100766_Rethinking_OODA_Toward_a_Modern_Cognitive_Framework_of_Command_Decision_Making/links/00463534dc13dd6f92000000/Rethinking-OODA-Toward-a-Modern-Cognitive-Framework-of-Command-Decision-Making.pdf.

86 Army Technology, "Radars, Reconnaissance and Software Are Shaping the Artillery War in Ukraine", 10 June 2022, https://www.army-technology.com/comment/radars-reconnaissance-and-software-are-shaping-the-artillery-war-in-ukraine/.

87 Pettyjohn, 2024.

88 V. Bergengruen, "How Tech Giants Turned Ukraine into an AI War Lab", *Time*, 8 February 2024, https://time.com/6691662/ai-ukraine-war-palantir/.

89 Ibid. In March 2024 Palantir also unveiled a deal with the Ukrainian Ministry of the Economy to assist it in demining operations; see https://investors.palantir.com/news-details/2024/Palantir-and-Ministry-of-Economy-of-Ukraine-Sign-Demining-Partnership/.

90 *The Economist*, "The Invasion of Ukraine Is Not the First Social Media War, but It Is the Most Viral", 2 April 2022, https://www.economist.com/international/the-invasion-of-ukraine-is-not-the-first-social-media-war-but-it-is-the-most-viral/21808456.

91 L. O'Carroll, "Meet Diia: The Ukrainian App Used to Do Taxes ... and Report Russian Soldiers", *The Guardian*, 26 May 2023, https://www.theguardian.com/world/2023/may/26/meet-diia-the-ukrainian-app-used-to-do-taxes-and-report-russian-soldiers.

92 G.C. Allen, "Across Drones, AI, and Space, Commercial Tech Is Flexing Military Muscle in Ukraine", Center for Strategic and International Studies, 13 March 2022, https://www.csis.org/analysis/across-drones-ai-and-space-commercial-tech-flexing-military-muscle-ukraine.

93 S. Bendett, "Role and Implications of AI in the Russian–Ukrainian Conflict", Russia Matters, 20 July, 2023, https://www.russiamatters.org/analysis/roles-and-implications-ai-russian-ukrainian-conflict.

94 S. Bendett, "Russia's Artificial Intelligence Boom May Not Survive the War", Defense One, 15 April 2022, https://www.defenseone.com/ideas/2022/04/russias-artificial-intelligence-boom-may-not-survive-war/365743/. C4ISR stands for command, control, communications, computers and intelligence surveillance and reconnaissance.

95 S. Bendett, "The Development of Artificial Intelligence in Russia", in N.D. Wright (ed.), *Artificial Intelligence, China, Russia, and the Global Order*, 2019, pp.168-177, https://www.jstor.org/stable/resrep19585.28#metadata_info_tab_contents.

[96] Ibid.

[97] M. Meaker, "Ukraine's War Brings Autonomous Weapons to the Front Lines", Wired, 24 February 2023, https://www.wired.co.uk/article/ukraine-war-autonomous-weapons-frontlines.

[98] Ibid.

[99] D. Hambling, "Ukrainian AI Attack Drones May Be Killing without Human Oversight", *New Scientist*, 13 October 2023, https://www.newscientist.com/article/2397389-ukrainian-ai-attack-drones-may-be-killing-without-human-oversight/. It must be noted that reports of fully autonomous drones are a feature of modern conflicts. In 2021 a controversial and disputed UN report described an incident in Libya where a Turkish Kargu-2 drone had reportedly pursued and engaged forces fully autonomously. For more information, see J. Vincent, "Have Autonomous Robots Started Killing in War?", The Verge, 3 June 2021, https://www.theverge.com/2021/6/3/22462840/killer-robot-autonomous-drone-attack-libya-un-report-context.

[100] D. Hambling, "Ukraine's AI Drones Seek and Attack Russian Forces without Human Oversight", Forbes, 17 October 2023, https://www.forbes.com/sites/davidhambling/2023/10/17/ukraines-ai-drones-seek-and-attack-russian-forces-without-human-oversight/?sh=40ad315766da.

[101] F. Farrell, "How Russia's Homegrown Lancet Drone Became so Feared in Ukraine", *Kyiv Independent*, 8 November 2023, https://kyivindependent.com/how-russias-homegrown-lancet-drone-became-so-feared-in-ukraine/.

[102] Z. Kallenborn and P.C. Bleek, "Drones of Mass Destruction: Drone Swarms and the Future of Nuclear, Chemical, and Biological Weapons", War on the Rocks, 14 February 2019, https://warontherocks.com/2019/02/drones-of-mass-destruction-drone-swarms-and-the-future-of-nuclear-chemical-and-biological-weapons/.

[103] E. Ackerman and J. Stavridis, "Drone Swarms Are About to Change the Military Balance of Power", *Wall Street Journal*, 14 March 2024, https://www.wsj.com/tech/drone-swarms-are-about-to-change-the-balance-of-military-power-e091aa6f.

[104] J. Wakefield, "Deepfake Presidents Used in Russia-Ukraine War", BBC, 18 March 2022, https://www.bbc.com/news/technology-60780142.

[105] J.-M. Rickli and M. Ienca, "The Security and Military Implications of Neurotechnology and Artificial Intelligence", in F. Orsolya et al. (eds), *Clinical Neurotechnology Meets Artificial Intelligence: Philosophical, Ethical, Legal and Social Implications*, 2021, pp.197-215, https://link.springer.com/content/pdf/10.1007/978-3-030-64590-8.pdf; S. Karnouskos, "Artificial Intelligence in Digital Media: The Era of Deepfakes", *IEEE Transactions on Technology and Society*, June 2020, https://www.researchgate.net/profile/Stamatis-Karnouskos/publication/342795647_Artificial_Intelligence_in_Digital_Media_The_Era_of_Deepfakes/links/5f2dc189458515b7290d312f/Artificial-Intelligence-in-Digital-Media-The-Era-of-Deepfakes.pdf; R. Chesney and D. Citron, "Deepfakes and the New Disinformation War", *Foreign Affairs*, January 2019, https://www.foreignaffairs.com/articles/world/2018-12-11/deepfakes-and-new-disinformation-war; R. Chesney and D. Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy and National Security", *California Law Review*, December 2019, https://scholarship.law.bu.edu/cgi/viewcontent.cgi?article=1640&context=faculty_scholarship.

[106] P. Sonne, "Fake Putin Speech Calling for Martial Law Aired in Russia", *New York Times*, 5 June 2023, https://www.nytimes.com/2023/06/05/world/europe/putin-deep-fake-speech-hackers.html.

[107] J.-M. Rickli, "Does the UN Need a Watchdog to Fight Deepfakes and Other AI Threats?", World Economic Forum, 2 August 2023, https://www.weforum.org/agenda/2023/08/does-un-needs-watchdog-fight-deepfakes-ai-threats/.

[108] P. Dave and J. Dastin, "Exclusive: Ukraine Has Started Using Clearview AI's Facial Recognition during War", Reuters, 14 March 2022, https://www.reuters.com/technology/exclusive-ukraine-has-started-using-clearview-ais-facial-recognition-during-war-2022-03-13/.

[109] F.-S. Gady and M. Kofman, "Making Attrition Work: A Viable Theory of Victory for Ukraine", *Survival*, Vol.66(1), 2024, pp.7-24, https://doi.org/10.1080/00396338.2024.2309068.

[110] Pettyjohn, 2024.

[111] Ibid. In the air defence domain Ukraine may have benefitted from the US Army's Integrated Battle Command System built by Northrop Grumman (and used by Poland), but this remains to be confirmed.

112 Santora, 4 February 2024.

113 C. Krebs, "The Cyber Warfare Predicted in Ukraine May Be Yet to Come", *Financial Times*, 20 March 2022, https://www.google.com/search?q=the+cyber+warfare+predicted+in+Ukraine+may+be+yet+to+come&oq=the+cyber+warfare+predicted+in+Ukraine+may+be+yet+to+come&aqs=chrome..69i57j69i64.1271j0j4&sourceid=chrome&ie=UTF-8.

114 CyberPeace Institute, *Cyber Dimensions of the Conflict in Ukraine*, Report, 2023, https://cyberconflicts.cyberpeaceinstitute.org/.

115 Ibid.

116 Ibid.

117 A. Greenberg, "How an Entire Nation Became Russia's Test Lab for Cyberwar", Wired, 20 June 2017, https://www.wired.com/story/russian-hackers-attack-ukraine/; J.A. Lewis, "Cyber War and Ukraine", Center for Strategic and International Studies, June 2022, https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/220616_Lewis_Cyber_War.pdf?S.iEKeom79InugnYWlcZL4r3Ljuq.ash.

118 A. Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History", Wired, 22 August 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

119 Lewis, 2022.

120 *The Economist*, "Lessons from Russia's Cyber-war in Ukraine", 30 November 2022, https://www.economist.com/science-and-technology/2022/11/30/lessons-from-russias-cyber-war-in-ukraine.

121 Lewis, 2022.

122 D. Sanger, "Once, Superpower Summits Were about Nukes. Now, Its Cyberweapons", *New York Times*, 15 June 2021, https://www.nytimes.com/2021/06/15/world/europe/biden-putin-cyberweapons.html.

123 M. Schulze, "Can Russia and the West Avoid a Major Cyber Escalation?", *National Interest*, 15 April 2022, https://nationalinterest.org/blog/techland-when-great-power-competition-meets-digital-world/can-russia-and-West-avoid-major-cyber.

124 B. Smith, "Defending Ukraine: Early Lessons from the Cyber War", Microsoft, 22 June 2022, https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/.

125 K. Duffy, "A Top Pentagon Official Said SpaceX Starlink Rapidly Fought off a Russian Jamming Attack in Ukraine", *Business Insider*, 22 April 2022, https://www.businessinsider.com/spacex-starlink-pentagon-russian-jamming-attack-elon-musk-dave-tremper-2022-4?r=US&IR=T.

126 Lewis, 2022.

127 S. Soesanto, "The IT Army of Ukraine: Structure, Tasking and Ecosystem", ETH Centre for Security Studies, June 2022, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2022-06-IT-Army-of-Ukraine.pdf; Krieg and Rickli, 2019.

128 Soesanto, 2022.

129 Ibid.

130 Soesanto, 2022.

131 Krieg and Rickli, 2019.

132 Ibid.

133 D. Milmo, "Anonymous: The Hacker Collective that Has Declared Cyberwar on Russia", *The Guardian*, 28 February 2022, https://www.theguardian.com/world/2022/feb/27/anonymous-the-hacker-collective-that-has-declared-cyberwar-on-russia.

134 Greenberg, 2018; J. Limnell, "Russian Cyber Activities in the EU", European Union Institute for Security Studies, 2018, https://www.jstor.org/stable/pdf/resrep21140.10.pdf?refreqid=excelsior%3A5c063e24a1bfcb3e1477e3e34c06516e&ab_segments=&origin=&acceptTC=1.

135 T. Rodenhäuser and M. Vignati, "8 Rules for 'Civilian Hackers' during War and 4 Obligations for States to

Restrain Them", ICRC, 4 October 2023, https://blogs.icrc.org/law-and-policy/2023/10/04/8-rules-civilian-hackers-war-4-obligations-states-restrain-them/.

136 E. Harding, "The Hidden War in Ukraine", Center for Strategic and International Studies, 15 June 2022, https://www.csis.org/analysis/hidden-war-ukraine.

137 L. Maschmeyer and M. Dunn Cavelty, "Goodbye Cyberwar: Ukraine as Reality Check", *Policy Perspectives*, Vol.10(3), May 2022, https://ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/PP10-3_2022-EN.pdf.

138 J.-M. Rickli and A. Kaspersen "The Global War of Narratives and the Role of Social Media", World Economic Forum Blog, 8 July 2016, https://www.weforum.org/agenda/2016/07/the-global-war-of-narratives-and-the-role-of-social-media/.

139 BBC, "Ukraine Anger as Macron Says 'Don't Humiliate Russia'", 4 June 2022, https://www.bbc.com/news/world-europe-61691816.

140 P. Baines, "Ukrainian Propaganda: How Zelensky Is Winning the Information War against Russia", The Conversation, 11 May 2022, https://theconversation.com/ukrainian-propaganda-how-zelensky-is-winning-the-information-war-against-russia-182061.

141 R. Cohen, "A Surge of Unifying Moral Outrage over Russia's War", *New York Times*, 1 March 2022, https://www.nytimes.com/2022/03/01/world/europe/zelensky-ukraine-war-outrage.html.

142 Stand For Ukraine, "Support Ukraine in the Face of Russian Aggression", accessed 10 July 2022, https://standforukraine.com/; Soesanto, 2022.

143 T. Gibbons-Neff, "Russia Regains Upper Hand in Ukraine's East as Kyiv's Troops Struggle", *New York Times*, 13 January 2024, https://www.nytimes.com/2024/01/13/world/europe/ukraine-russia-war.html.

144 *The Guardian*, "Troll Factory Spreading Russian Pro-war Lies Online, Says UK", 1 May 2022, https://www.theguardian.com/world/2022/may/01/troll-factory-spreading-russian-pro-war-lies-online-says-uk.

145 Viginum, *Portal Kombat: A Structured and Coordinated Pro-Russian Propaganda Network*, Premier Ministre, February 2024, https://www.sgdsn.gouv.fr/files/files/Publications/20240214_NP_SGDSN_VIGINUM_PORTAL-KOMBAT-NETWORK_PART2_ENG_VF.pdf.

146 V. Jack, "Russia Expands Laws Criminalizing 'Fake News'", *Politico*, 22 March 2022, https://www.politico.eu/article/russia-expand-laws-criminalize-fake-news/.

147 Debunk.org, "Kremlin Spent 1.9 Billion USD on Propaganda Last Year, the Budget Exceeded by a Quarter", 4 May 2023, https://www.debunk.org/kremlin-spent-1-9-billion-usd-on-propaganda-last-year-the-budget-exceeded-by-a-quarter.

148 A. Satariano, "How Russia Took Over Ukraine's Internet in Occupied Territories", *New York Times*, 9 August 2022, https://www.nytimes.com/interactive/2022/08/09/technology/ukraine-internet-russia-censorship.html.

149 C. Miller, "Who's Behind #IStandWithPutin?", *The Atlantic*, 5 April 2022, https://www.theatlantic.com/ideas/archive/2022/04/russian-propaganda-zelensky-information-war/629475/.

150 Al Jazeera, "Kremlin Denies Blame for Food Crisis as Putin Meets AU Leaders", 3 June 2022, https://www.aljazeera.com/news/2022/6/3/kremlin-denies-blame-for-mounting-food-crisis-as-putin-meets-african-union-leaders.

151 J. Crawford, "Russia's War in Ukraine Highlights UN Fault Lines", Swissinfo, 8 April 2022, https://www.swissinfo.ch/eng/politics/russia-s-war-in-ukraine-highlights-un-fault-lines/47496526.

152 J. Psaropoulos, "Russian Diplomacy Leverages Israel Hamas War for Moral High Ground", Al Jazeera, 20 November 2023, https://www.aljazeera.com/news/2023/11/20/russian-diplomacy-leverages-israel-hamas-war-for-moral-high-ground; N. Smagin, "Gaza Convinced Russia It Was Right All Along", Carnegie Endowment for International Peace, 7 December 2023, https://carnegieendowment.org/politika/91189.

153 *The Economist*, 2 April 2022.

154 C. Albon, "How Commercial Space Systems Are Changing the Conflict in Ukraine", *C4ISRNET*, 25 April

2022, https://www.c4isrnet.com/intel-geoint/2022/04/25/how-commercial-space-systems-are-changing-the-conflict-in-ukraine/.

[155] C. Perez and A. Nair, “Information Warfare in Russia’s War in Ukraine”, *Foreign Policy*, 22 August 2022, https://foreignpolicy.com/2022/08/22/information-warfare-in-russias-war-in-ukraine/.

[156] J.-M. Rickli, “(Dis)information as a Tool of Warfare”, Geneva Graduate Institute Podcast, April 2023, https://soundcloud.com/ro_iheid/disinformation-as-a-tool-of-warfare.

[157] Zabrodskyi et al., 2022.

[158] Ibid.

[159] Ibid.

[160] Ibid.

[161] R. Lee, “The Tank Is Not Obsolete, and Other Observations about the Future of Combat”, War on the Rocks, 6 September 2022, https://warontherocks.com/2022/09/the-tank-is-not-obsolete-and-other-observations-about-the-future-of-combat/.

[162] Watling and Reynolds, 19 May 2023.

[163] L. Jakes et al., “After Suffering Heavy Losses, Ukrainians Paused to Rethink Strategy”, *New York Times*, 15 July 2023, https://www.nytimes.com/2023/07/15/us/politics/ukraine-leopards-bradleys-counteroffensive.html.

[164] Ibid.

[165] Russia Matters, “The Russia-Ukraine War Report Card, Jan. 2, 2024”, 2 January 2024, https://www.russiamatters.org/blog/russia-ukraine-war-report-card-jan-2-2024; J. Janovsky et al., “Attack on Europe: Documenting Russian Equipment Losses during the Russian Invasion of Ukraine”, Oryx, 24 February 2022, https://www.oryxspioenkop.com/2022/02/attack-on-europe-documenting-equipment.html.

[166] Ibid.; Russia Matters, 2 January 2024.

[167] Estonia, Ministry of Defence, “Russia’s War in Ukraine: Myths and Lessons”, January 2023, https://kaitseministeerium.ee/sites/default/files/myths_and_lessons_0.pdf.

[168] P. Stewart, “Russia Ramps up Artillery Production but Still Falling Short, Western Official Says”, Reuters, 9 September 2023, https://www.reuters.com/world/europe/russia-ramps-up-artillery-production-still-falling-short-western-official-says-2023-09-09/.

[169] H. Foy, “Ukraine War Is “Battle for Ammunition”, Says NATO Chief”, *Financial Times*, 23 January 2024, https://www.ft.com/content/0c270033-3340-4e76-ac45-8eaf77514365.

[170] P. Tucker, “The West Is Underestimating Ukraine’s Artillery Needs”, Defense One, 22 February 2024, https://www.defenseone.com/business/2024/02/west-underestimating-ukraines-artillery-needs/394392/.

[171] Watling, 3 January 2024.

[172] V. de Graffenried, “Et si l’Europe achetait des munitions à l’inde ou à l’Afrique du Sud pour les envoyer à Kiev ?”, *Le Temps*, 4 March 2024, https://www.letemps.ch/monde/et-si-l-europe-achetait-des-munitions-a-l-inde-ou-a-l-afrique-du-sud-pour-les-envoyer-a-kiev; S. Skove, “In Race to make Artillery Shells, US, EU, See Different Results”, Defense One, 27 November 2023, https://www.defenseone.com/business/2023/11/race-make-artillery-shells-us-eu-see-different-results/392288/.

[173] It is also worth noting that Ukraine also faces critical challenges to mobilise more soldiers at the beginning of 2024; see Santora, 24 February 2024.

[174] Ibid.

[175] Pettyjohn, 2024.

[176] Ibid.

[177] E. Court, “Deputy Minister: Ukraine Can Produce 150,000 Drones per Month”, *Kyiv Independent*, 5 March 2024, https://kyivindependent.com/deputy-minister-ukraine-can-produce-150-000-drones-per-month/;

S. Bendett, https://twitter.com/sambendett/status/1763914626364817724.

178 S. Cranny-Evans, "Russia's Artillery War in Ukraine: Challenges and Innovations", RUSI, 9 August 2023, https://rusi.org/explore-our-research/publications/commentary/russias-artillery-war-ukraine-challenges-and-innovations.

179 D. Sanger et al., "A New Concern on the Ukrainian Battlefield: North Korea's Latest Missiles", *New York Times*, 22 January 2024, https://www.nytimes.com/2024/01/22/us/politics/russia-ukraine-north-korea.html.

180 S. Egeli, "Emerging and Disruptive Technologies in Russia's War against Ukraine", in A. Vicente et al. (eds), *Russia's War on Ukraine: Contributions to Political Science*, Springer, 2023, https://doi.org/10.1007/978-3-031-32221-1_5.

181 J. Watling and N. Reynolds, "Stormbreak: Fighting through Russian Defences in Ukraine's 2023 Offensive", RUSI, September 2023, https://static.rusi.org/Stormbreak-Special-Report-web-final_0.pdf.

182 Ibid.

183 F. Borsari, "The Tank's Death Has Been Exaggerated", Center for European Policy Analysis, 24 June 2022, https://cepa.org/article/the-tanks-death-has-been-exaggerated/.

184 Ibid.

185 J.Q. Bolton, "The More Things Change ... Russia's War in Ukraine Mirrors the Past as Much as It Shows the Future", *Military Review*, July 2023, https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/Online-Exclusive/2023/The-More-Things-Change/Bolton-AWC-Ukraine-Observations-UA.pdf.

186 *The Economist*, "A Stunning Counter-offensive by Ukraine's Armed Forces", 15 September 2022, https://www.economist.com/europe/2022/09/15/a-stunning-counter-offensive-by-ukraines-armed-forces.

187 J. Gettleman and A.E. Kramer, "In Reclaimed Towns, Ukrainians Recount a Frantic Russian Retreat", *New York Times*, 13 September 2022, https://www.nytimes.com/2022/09/13/world/europe/ukraine-russia-retreat-morale.html.

188 Gady and Kofman, 2024.

189 *The Economist*, 5 February 2024.

190 Ibid.

191 Ibid.

192 Gady and Kofman, 2024.

193 *Washington Post*, 4 December 2023.

194 Gady and Kofman, 2024, pp.7-24.

195 Ibid.

196 J. Watling, "Ukraine Must Prepare for a Hard Winter", RUSI, 19 October 2023, https://www.rusi.org/explore-our-research/publications/commentary/ukraine-must-prepare-hard-winter.

197 F. Farrell, "Ukraine Struggles to Ramp up Mobilization as Russia's War Enters 3rd Year", *Kyiv Independent*, 23 January 2024, https://kyivindependent.com/move-to-expand-mobilization-brings-ukrainian-society-face-to-face-with-immense-pressure-of-war/.

198 N. Bagirova, "Exclusive: After Ukraine, 'Whole World' Is a Customer for Turkish Drone, Maker Says", Reuters, 20 May 2022, https://www.reuters.com/business/aerospace-defense/exclusive-after-ukraine-whole-world-is-customer-turkish-drone-maker-says-2022-05-30/.

199 L. Harding, "Cheap but Lethally Accurate: How Drones Froze Ukraine's Frontlines", *The Guardian*, 25 January 2024, https://www.theguardian.com/world/2024/jan/25/how-drones-froze-ukraine-frontlines.

200 Borsari and Davis, 2023.

201 N. Reynolds and J. Watling, "Ukraine at War: Paving the Road from Survival to Victory", RUSI, 4 July 2022, https://rusi.org/explore-our-research/publications/special-resources/ukraine-war-paving-road-survival-victory.

[202] A. Calcara et al., “Why Drones Have Not Revolutionized War”, *International Security*, Vol.46(4), 2022, pp.130-171, https://iris.luiss.it/bitstream/11385/217877/1/2022Calcara-Gilli-etal.pdf.

[203] Ibid.

[204] Kunertova, 2023.

[205] *The Economist*, 5 February 2024.

[206] Ibid.

[207] Robinson, 2022.

[208] Rickli et al., 2023.

[209] A. Vershinin, “The Return of Industrial Warfare”, RUSI, 17 June 2022, https://www.rusi.org/explore-our-research/publications/commentary/return-industrial-warfare.

[210] J.-M. Rickli, “The Strategic Implications of Artificial Intelligence”, in A. Naqvi and J.M. Munoz (eds), *Handbook of Artificial Intelligence and Robotic Process Automation: Policy and Government Applications*, Anthem Press, 2020.

[211] J.-M. Rickli and F. Mantellassi, "Human-Machine Teaming in Artificial Intelligence-driven Air Power", *Air Power Journal*, Fall 2022, https://www.diacc.ae/resources/2022_Jean_Marc_Rickli_Federico_Mantellassi_Human-Machine_Teaming_Air_Power.pdf.

[212] Kunertova, 2023.

[213] C.S. Gray, *Modern Strategy*, Oxford University Press, 1999.

[214] Kunertova, 2023.

[215] M. Ryan, “Russia’s Adaptation Advantage”, *Foreign Affairs*, 5 February 2024, https://www.foreignaffairs.com/ukraine/russias-adaptation-advantage.

[216] A. Azar, *Exponential: Order and Chaos in an Age of Accelerating Technology*, Penguin Random House, 2021.

[217] J.-M. Rickli et al., “What, Why and When? A Review of the Key Issues in the Development and Deployment of Military Human-Machine Teams”, Tailored Study, Geneva Centre for Security Policy, February 2024, https://dam.gcsp.ch/files/doc/what-why-and-when-a-review-of-the-key-issues-in-the-development-and-deployment-of-military-human-machine-teams?.

Geneva Papers Research Series

No.1 2011 G. P. Herd, “The Global Puzzle: Order in an Age of Primacy, Power-Shifts and Interdependence”, 34p.

No.2 2011 T. Tardy, “Cooperating to Build Peace: The UN-EU Inter-Institutional Complex”, 36p.

No.3 2011 M.-M. Ould Mohamedou, “The Rise and Fall of Al Qaeda: Lessons in Post-September 11 Transnational Terrorism”, 39p.

No.4 2011 A. Doss, “Great Expectations: UN Peacekeeping, Civilian Protection and the Use of Force”, 43p.

No.5 2012 P. Cornell, “Regional and International Energy Security Dynamics: Consequences for NATO’s Search for an Energy Security Role”, 43p.

No.6 2012 M.-R. Djalili and T. Kellner, “Politique Régionale de l’Iran: Potentialités, Défis et Incertitudes”, 40p.

No.7 2012 G. Lindstrom, “Meeting the Cyber Security Challenge”, 39p.

No.8 2012 V. Christensen, “Virtuality, Perception and Reality in Myanmar’s Democratic Reform”, 35p.

No.9 2012 T. Fitschen, “Taking the Rule of Law Seriously”, 30p.

No.10 2013 E. Kienle, “The Security Implications of the Arab Spring”, 32p.

No.11 2013 N. Melzer, “Human Rights Implications of the Usage of Drones and Unmanned Robots in Warfare”, 75p.

No.12 2013 A. Guidetti et al., ‘’World Views: Negotiating the North Korean Nuclear Issue”, 47p.

No.13 2013 T. Sisk and M.-M. Ould Mohamedou, “Bringing Back Transitology: Democratisation in the 21st Century”, 36p.

No.14 2015 H. J. Roth, “The Dynamics of Regional Cooperation in Southeast Asia”, 35p.

No.15 2015 G. Galice, “Les Empires en Territoires et Réseaux”, 42p.

No.16 2015 S. C. P. Hinz, “The Crisis of the Intermediate-range Nuclear Forces Treaty in the Global Context”, 36p.

No.17 2015 H. J. Roth, “Culture – An Underrated Element in Security Policy”, 40p.

No.18 2016 D. Esfandiary and M. Finaud, “The Iran Nuclear Deal: Distrust and Verify”, 44p.

No.19 2016 S. Martin, “Spying in a Transparent World: Ethics and Intelligence in the 21st Century”, 42p.

No.20 2016 A. Burkhalter, “Définir le Terrorisme: Défis et Pratiques”, 50p.

No.21 2017 M. Finaud, “‘Humanitarian Disarmament’: Powerful New Paradigm or Naive Utopia?”, 48p.

No.22 2017 S. Aboul Enein, “Cyber Challenges in the Middle East”, 49p.

No.23 2019 Tobias Vestner, “Prohibitions and Export Assessment: Tracking Implementation of the Arms Trade Treaty”, 28p.

No.24 2019 Mathias Bak, Kristoffer Nilaus Tarp and Dr. Christina Schori Liang, “Defining the Concept of ‘Violent Extremism’”, 32p.

No.25 2020 Cholpon Orozobekova and Marc Finaud, “Regulating and Limiting the Proliferation of Armed Drones: Norms and Challenges”, 47p.

No.26 2020 Dr Gervais Rufyikiri, “Reshaping Approaches to Sustainable Peacebuilding and Development in Fragile States – Part I: Nexus between Unethical Leadership and State Fragility", 47p.

No.27 2020 Dr Gervais Rufyikiri, “Reshaping Approaches to Sustainable Peacebuilding and Development in Fragile States – Part II: Nexus between Unethical Leadership and State Fragility", 44p.

No.28 2021 Dr Gervais Rufyikiri, "Resilience in Post-civil War, Authoritarian Burundi: What Has Worked and What Has Not?”, 47p.

No.29 2022 Kevin M. Esvelt, "Delay, Detect, Defend: Preparing for a Future in which Thousands Can Release New Pandemics”, 65p.

No.30 2023 Stuart Casey-Maslen, “International Counterterrorism Law: Key Definitions and Core Rules”, 40p.

No.31 2023 Anjali Gopal, William Bradshaw, Vaishnav Sunil and Kevin M. Esvelt, “Securing Civilisation Against Catastrophic Pandemics”, 50p.

No.32 2024 Kemal Mohamedou, “The Wagner Group, Russia's Foreign Policy and Sub-Saharan Africa”, 41p.

No.33 2024 Anila Jelesijević, “The Prospective of the Western Balkans to the EU membership: Challenges and Possible Ways Forward”, 40p.

Building Peace Together

Geneva Centre for Security Policy
Maison de la paix
Chemin Eugène-Rigot 2D
P.O. Box 1295
1211 Geneva 1
Switzerland
Tel: + 41 22 730 96 00
E-mail: info@gcsp.ch
www.gcsp.ch

ISBN: 978-2-88947-122-5

GCSP
Geneva Centre for
Security Policy