CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

Swedish
Defence
University

The Digital in War: From Innovation to Participation

Steve Feldstein and Matthew Ford, editors

Nate Allen | Rupert Barrett-Taylor | Emily Bienvenue | Mirjam de Bruijn
Maryanne Kelton | Kristin Ljungkvist | Jack McDonald | Jethro Norman
Zac Rogers | Michael Sullivan | Gavin Wilde

The Digital in War: From Innovation to Participation

Steve Feldstein and Matthew Ford, editors

Nate Allen | Rupert Barrett-Taylor | Emily Bienvenue | Mirjam de Bruijn
Maryanne Kelton | Kristin Ljungkvist | Jack McDonald | Jethro Norman
Zac Rogers | Michael Sullivan | Gavin Wilde

Carnegie Endowment for International Peace
Publications Department
1779 Massachusetts Avenue NW
Washington, D.C. 20036
P: + 1 202 483 7600
F: + 1 202 483 1840
CarnegieEndowment.org

This publication can be downloaded at no cost at CarnegieEndowment.org

Contents

00

Introduction

Steve Feldstein and Matthew Ford

The world is living through a period of extraordinary technological disruption in warfare. The war in Ukraine has become one of the most consequential laboratories of conflict in the twenty-first century, and its effects are reverberating far beyond Europe. It is a war not only fought with tanks, artillery, and soldiers, but also with codes, networks, drones, smartphones, and the ingenuity of ordinary people.[1] This fusion of state power, citizen participation, and rapid technological innovation is transforming how society thinks about war, strategy, and even sovereignty itself.

The Ukraine war has imparted a series of vital lessons that have unsettled the default assumptions of military strategists across the globe. For much of the modern era, size and resources defined military power. Large, well-funded militaries—those that could amass sophisticated fleets, long-range missiles, and heavy ground forces—were assumed to hold overwhelming advantages against weaker opponents. Yet Ukraine has repeatedly shown that nimbleness and adaptation can offset brute force. The defeat of Russia's Black Sea Fleet using domestically built sea drones is emblematic of this shift. Ukrainians leveraged local innovation, cheap materials, and agile thinking to neutralize a cornerstone of Russian naval power.

This dynamic represents a new paradigm: the emergence of "good enough" systems that are cheap, attritive, and lethal. Unlike the exquisite, high-cost weapons platforms of the past—such as jet fighters, guided missile destroyers, and armored divisions—these systems do not aspire to perfection. They are built to be expendable, to swarm, to overwhelm, and to adapt faster than traditional procurement cycles can respond. A drone that costs a few thousand dollars but can disable a million-dollar tank represents a radical rebalancing of military economics. Attritability has become an asset rather than a liability.

Perhaps most unsettling for traditional strategists is the blurring of the line between citizens and combatants. Driven by innovations like smartphones and encrypted messaging apps, war has become increasingly networked and participatory. Civilians with coding skills, 3D printers, or access to consumer drones can make meaningful contributions to the battlefield.

Soldiers use smartphones for reconnaissance, targeting, and real-time communication; volunteers map enemy positions using open-source intelligence; and diaspora communities crowdfund equipment and technology for the front. The neat boundaries of "front line" and "rear area," "soldier" and "civilian," have eroded.

The consequences extend far beyond Ukraine's borders. Other conflicts are now seeing the rapid importation of these practices, altering battlefield behavior and reshaping the character of war. Consider Myanmar, where the ongoing struggle between the Karenni Nationalities Defense Force (KNDF) and the military junta demonstrates the global diffusion of wartime innovation.[2]

When fighting erupted, the KNDF faced staggering resource disadvantages compared to the government military. Yet, rather than succumb, the rebels turned to the technologies at hand. They assembled a drone force from 3D-printed frames, old agricultural drones from China, and scavenged components from unrelated devices. The drone operators were not trained pilots but young, tech-savvy volunteers who had honed their skills on Discord, Telegram, and YouTube. Over time, they incorporated imported commercial quadcopters and first-person view drones, but their force remained a patchwork of improvisation.

Despite these constraints, the rebel drone units inflicted significant damage on government forces, demonstrating again that innovation and agility could offset raw firepower. Yet the cycle of adaptation did not stop there. The junta responded by building its own drone capacity, leaning on Chinese and Russian imports as a backbone. Unlike the rebels' cobbled-together systems, the government produced higher-capacity devices, imported specialized surveillance and attack drones, developed customized bombs, and formally integrated drone training into its military structure—preserving air superiority.[3] Today, four years into the conflict, drones have become "a ubiquitous presence." Myanmar now ranks third globally for drone events, behind only Ukraine and Russia.[4]

This case highlights not only the diffusion of battlefield technologies but also the accelerating tempo of military adaptation. What emerges in one conflict is quickly studied, copied, and modified in another. No innovation remains the exclusive property of one side for long. Myanmar's rebels and junta are locked into the same cycle of experimentation, escalation, and counter-innovation that defines the Ukrainian battlefield.

These dynamics underscore a broader transformation: War is no longer bounded by geography or by the monopoly of states. The smartphone has become one of the most consequential weapons of the modern era. It allows soldiers to live stream combat, civilians to track troop movements, and diasporas to coordinate fundraising campaigns. Social media platforms transform battles into global spectacles, shaping international perceptions in real time. Apps like Telegram blur the line between operational communication and propaganda dissemination. A war fought on smartphones is both a military contest and a battle of narratives.

This introduction to our collection of articles situates Ukraine as the pacesetter in this new age of networked, technologically disrupted warfare—but it also insists on a wider view. The patterns emerging in Ukraine are neither isolated nor anomalous, with impacts ranging from the forests of Myanmar to the deserts of the Middle East and from the South China Sea to cyberspace. They are part of a global shift in the conduct of war.

The articles in this collection probe this disruption from multiple angles. Some focus on the battlefield, examining the technologies and tactics that have emerged from Ukraine and spread elsewhere. Others step back to analyze the social, political, and ethical implications of a world in which civilians become combatants, smartphones become weapons, and attrition becomes a design principle. Still others place these innovations in historical perspective, asking how this moment compares to earlier technological revolutions in warfare—such as the machine gun, the tank, and the nuclear bomb.

Together, these articles chart a world in flux. They show how the improvisational creativity of Ukrainian engineers, Burmese rebels, and other countless civilians has reshaped the terrain of conflict. They explore the consequences for great powers who find their expensive platforms vulnerable to cheap, swarming adversaries. They examine the implications for international law and expose a deeper failure: The laws of war have not kept pace with new developments. International humanitarian law was designed to protect civilians, regulate combatants, and constrain violence, but the emergence of drones, AI-enabled systems, and participatory conflict strains its applicability. When civilians operate drones, provide targeting data, or engage in cyber operations, are they lawful combatants or illegitimate participants? Who bears responsibility for lethal outcomes in a world of semiautonomous systems? The growing gap between innovation and regulation leaves both militaries and societies in uncertain legal terrain.

We open this collection with an article about Ukraine because it has crystallized the dynamics of this new era. But the journey does not end there. By tracing the diffusion of innovation to other regions and locales and by examining the interplay of technology, society, and strategy across regions, we aim to illuminate the contours of a truly global transformation.

The Digital in War

These articles grew out of conversations about changes originating on the battlefield. We organized a workshop in January 2024 where we debated these questions and analyzed their impacts. Stemming out of these discussions, we assembled a collection of pieces to provide essential insights about the evolving nature of modern war.

Rupert Barrett-Taylor and Gavin Wilde kick off our series with their article, "A Digitized, Efficient Model of War."[5] In their piece, they critique an "overly reductive model of war," one that is techno-centric and built upon optimization and efficiency but arguably risks

undermining pragmatism and impact. They examine whether it is possible for modern militaries to resist the temptation to fit warfighting into machinery rather than to use machinery to reflect actual conditions on the ground and on the battlefield.

Nate Allen's article, "Digital Technology, Strategic Adaptation, and the Outcomes of Twenty-First Century Armed Conflict,"[6] poses a thorny question: If digital technology is bringing battlefield transformation, why are these innovations not leading to decisive victories? He argues that today's military innovations are rooted in an open technological ecosystem spurred by private companies and characterized by rapid cycles of innovation, adaptation, and readaptation. Allen looks at conflicts in Ukraine and Nigeria and observes how innovation-adaptation cycles explain why these conflicts appear stalemated "despite digital technology's ubiquity and proliferation."

Aurel Sari turns his focus to how digital technologies are reshaping the legal landscape in "War and Law in a Digital World."[7] Sari argues that as technological innovation alters battlefield realities, the lack of consensus about how existing rules apply risks turning legal arguments into extensions of conflicts. He acknowledges that the "increased reach, tempo, destructiveness, and availability of conventional force is now married to the ubiquity, speed, scale, and impact of measures short of war, including in the digital and information spheres." However, he rejects the contention that these developments have fully collapsed the combatant-civilian divide.

Jethro Norman offers an ethnographic perspective to modern war in "Foreign Fighters 2.0: The Interplay of Technology and Lived Experience in the Russia-Ukraine War."[8] He investigates how digital technologies are reshaping foreign fighter participation in contemporary warfare and attracting individuals with technical expertise rather than conventional combat backgrounds. He argues that these emergent participants "embody a convergence of civilian technical expertise and military operations, potentially redefining conventional boundaries between combatants and civilians."

In "Digital Connectivity and Digital Informants in War,"[9] Jack McDonald describes how smartphones and associated technologies permit any civilian to potentially pass targeting data to local and distant forces almost instantaneously. As a result, analysts must rethink how "intangible contributions to armed conflict" may expose civilians to targeting or heighten the risk that military forces violate international humanitarian law in response to digital informants.

Kristin Ljungkvist examines Sweden's Cold War–era strategy of total defense, which its government is in the process of reestablishing. She cautions in her article, "Participatory War and Its Challenges for Total Defense,"[10] that the ubiquity of digital networks and smart devices in today's environment poses unique challenges to this concept, raising questions about "civilian protection, trust in public institutions, and the upholding of democratic principles." Ljungkvist argues that as governments promote these precepts, they must reckon with difficult issues, such as the potential diminishment of civil liberties and the unpredictability of digitally mobilized populations.

In her article, "Digital Communication as a Weapon: The Case of Mali,"[11] Mirjam de Bruijn explores the role of digital communication networks in contributing to cultural violence in the ongoing war in Mali. Incorporating results from several research projects she has carried out in Mali and across the Sahel, de Bruijn looks at the digital dimensions of conflict, from social media platforms to cross-regional and transnational digital networks, internet and social media shutdowns, and digital propaganda.

Finally, Emily Bienvenue et al. analyze "Private Tech Companies, the State and the New Character of War."[12] In their article, the authors explore how private technology firms are renegotiating the state's sovereign control over military power. Unlike traditional defense contractors that supplied discrete hardware, contemporary tech companies such as Palantir, SpaceX, and commercial data platforms now manage the digital infrastructures, analytics, and AI systems upon which command and control depend. This is blurring the boundary between state and market authority. This new dependency signals a shift in the character of armed conflict, as states must navigate a global "war ecology" in which civilian technologies, venture capital imperatives, and transnational data networks increasingly coproduce both the means and meaning of war.

The age of technological disruption in warfare is here. It is not coming in the future; it is not confined to laboratories or think tanks. It is unfolding before our very eyes across battlefields. This collection is an invitation to grapple with that reality: to analyze it, to understand it, and to consider what it means for the wars yet to come.

01

A Digitized, Efficient Model of War

Rupert Barrett-Taylor and Gavin Wilde

Battlefields from Ukraine to Gaza have recently been marked, as have many conflicts over the last two decades, by the extensive use of airborne assets, surveillance, and computing power in pursuit of victory. Both precision guided weapons and unmanned vehicles create new and heavy demands on training and logistics, as well as whole organizational structures devoted to finding targets. In this regard, the datafication of the battlefield and the automation of targeting has reached a modern-day zenith, on the heels of decades of theorizing about "information dominance" in warfare.

However, this digital-age collection and targeting process is founded on a premise of fierce optimization and brutal efficiency. The resulting model of warfare is both a product of physical observation and digital construction. It is process-driven, techno-centric, and ultimately premised on being entirely calculable. A model of warfare which demands efficiency above all else not only risks fostering a disregard for pragmatism and efficacy, but is also arguably a subtle cover for the exercise of institutional power and control. This article critiques an overly reductive model of war, in the context of increasing demands for greater automation and applications of artificial intelligence (AI) which are widely presumed to be fixtures in future conflict.

(Efficient) War, What is it Good For?

Since at least the 1950s, availability of large-scale computing has enabled a culture in which organizations, including militaries, manage complexity by seeking underlying, generalizable laws governing their disciplines, relying on quantification and data processing to do so.[13] Each organization selects what they consider to be the most appropriate data and processing methods in the hope that computation yields competitive advantage. The underlying

assumption is that the adoption of these forms of technology improve efficiency and optimize the tasks of any organization.[14] However, this idea rests on a series of contestable beliefs about technology. While marginal in many arenas, there is significant danger in relying too casually on these assumptions in others. For example, large language models (LLMs) and their derivative products have been known to produce unreliable results to queries.[15] At the other end of the spectrum: the tragic wrestle between the autopilot and very human pilots on Lion Air flight 610 that ultimately cost almost 200 people their lives. Such cases may be exceptional, but they share a common thread: "the system was responding to faulty data."[16]

In the military domain, there is a long history of belief in the power of digital representation, matched to similar cautionary evidence of the dangers inherent to this belief. Technological advances in the Digital Era promised to deliver a toolkit for *efficiency* to military actors, economizing time and labor, and ultimately saving blood and treasure, while still accomplishing strategic goals.[17] Using digital representations in a repeatable process-based framework allows optimization and minimization of friction. In turn this allows wastage to be eliminated, and the speed of military operations to increase. This apes private sector responses to an economic model based on fierce market competition. Computation has thus been situated at the heart of warfare, but the consequences of a drive to efficiency are underestimated. Moreover, what is often unappreciated is the foundations for this model of warfare were laid even before the development of the digital computer, and it is arguable that the current model reliant on computing has only accelerated existing preferences.

Intra-military competition for a dominant warfighting paradigm echoes the tug-of-war between an *empirical* perspective and an imperial one, as characterized by political scientist James C. Scott: "The relation between scientific knowledge and practical knowledge is . . . part of a political struggle for institutional hegemony by experts and their institutions." In this regard, efforts to digitize the battlefield are "not just strategies of production, but also strategies of control and appropriation."[18] Thus, by excluding the unmeasurable and nondigitized qualities of the environment, the reification of targeting protects the pursuit of efficiency but also excludes insights that might prompt institutional introspection about accomplishing predefined goals. This risks what former UK signals intelligence chief David Omand warned about, an institutionalized tendency to become "better at counting examples of [digital] human behavior than critically explaining why they are and what it might mean."[19] Insofar as Elting Morison's observation that military organizations are "societies built around prevailing weapons systems," the targeting process may become primarily a means to exert influence within these societies—but this may or may not intersect with victory over an enemy in battle.[20]

As far back as the 1920s, enthusiastic supporters of airpower sought to show how it could defeat a future enemy through systematic bombardment of industrial infrastructure. However, assessments of Second World War strategic bombing against Germany indicate it would not have been successful by itself without the ground campaign in Europe.[21] During

the 1960s and 1970s the same ideas were linked by the U.S. Air Force to the power of digital computing. Computing was applied by U.S. forces against the North Vietnamese supply system during the Vietnam War by processing data gathered from sensors in the jungles of Laos.[22] This expensive and highly technical project was, at best, mildly successful, and easily spoofed by the enemy on the ground. Nonetheless, and despite a lack of conclusive evidence that systematic targeting resulted in concrete effects against enemies by the end of the Cold War, NATO had built a suite of collection and processing capabilities to survey and digitally represent the battlefield.[23] It remained anchored in a doctrine that sought to systematically target Soviet military forces, their logistics and their strategic infrastructure beyond the immediate battlefield. However the Soviets may have perceived these capabilities, amending their own planning and technological development in response, this datafied, mechanistic view of warfare remained largely speculative yet ceaselessly pursued by Western forces.

As far back as the 1920s, enthusiastic supporters of airpower sought to show how it could defeat a future enemy through systematic bombardment of industrial infrastructure.

Over time, the resulting Air-Land Battle doctrine became the later and better-known Revolution in Military Affairs, and remained the foundation of modern doctrine right up to its application against insurgents and terrorists throughout the Global War on Terror.[24] Operation Desert Storm, in which U.S. precision targeting against key decisionmakers and nodes ostensibly proved decisive, served as a testbed for the theory. The promise of quicker victories, fewer fires, and fewer casualties thanks to superior technology has since proven broadly alluring: U.S. precision munitions comprised 8 percent of U.S. fires in the Gulf War; 29 percent of NATO fires in Kosovo; by the Iraq War in 2003, this number had climbed to 68 percent.[25]

However, the era of uncontested U.S. military hegemony was arguably a false dawn—application of the same methods and ideas over the next twenty years would highlight the problems and flaws in this set of doctrinal ideas. The question of whether targeting a digital representation of the enemy results in strategic victory over any opponent remains open, while the contribution of so-called precision fires to wartime objectives is disputed. For instance, precision strikes in the Iraq War failed to achieve their objective of eliminating senior Iraqi leaders, killing over 100 civilian bystanders in the process;[26] industrial scale targeting of the digital representation of insurgency in Afghanistan for example did not significantly degrade its ultimate ability to retake the country.[27] Despite the AI-enabled targeting used by Israeli forces in Gaza, the destruction by late 2023 was nevertheless comparable to twice that of the Hiroshima bombings in 1945.[28] The attending civilian casualties, collateral damage, and propaganda aspects of such "precision" at scale are all too often dismissed.[29]

In Ukraine, targeting plays an adjunct role which is arguably more performative and supportive than by itself likely to defeat Russian forces relying heavily on mass.[30] However, targeted precision strike fits Western expectations of what factors determine success in war. These expectations reflect cultures of engineering-led innovation and economic competition rather than territorial defense or conquest. From digital representations of the battlefield emerge targets created from mountains of information, processed through socio-technical systems exploiting multiplicities of software and algorithms. Conventional wisdom driven by economics, expectations of technology and the promise of efficiency offered by computing place an emphasis on narratives of speed and efficiency. Faster computers and better optimized systems should lead to a prioritized array of targets, which should, in theory, represent a direct path to the destruction of the enemy's ability to wage war. The question remains, however, why this model has not already led to the collapse of Russian defenses or a capitulation by Hamas, as these conflicts drag on with little end in sight. The net outcome of heavy investment in techno-surveillance still appears to be measured in terms of body count and attrition of materiel on both sides. Contrary to the aspirations, precision has, on its own, yet to identify the *schwerpunkt promised by data-led military concepts.*

Absolutely Nothing (Except Control)

As noted by historian Simon Winchester, a preference for precision over accuracy means the "outcome may not necessarily reflect the true value of the desired end . . . accuracy is true to intention; precision is true to itself."[31] Take, for example, a Swiss-engineered wrist watch: it may keep time down to fractions of a second, but such precision is of no use if the clock is set three hours behind. The relationship and distinction between precision and accuracy, efficiency and efficacy, only become more blurry and complex with the introduction of new technologies and organizational imperatives.

By extension, Western attitudes toward technology and warfare are largely founded on the *positivist* nature of technological enquiry, which leads to digital construction of the battlefield primarily from data that can be measured and observed—which represent entities presumably behaving according to some underlying fixed, universal laws.[32] Data is then transformed through linear processes to constitute a discernable, digital world rather than attempting to translate the complex, physical phenomenon of conflict.[33] Underlying this is a cultural presumption that human subjectivity can be hedged against by relying instead upon more "raw" and thus ostensibly more objective data.[34] Yet, warfare is unavoidably both material *and* social. It is subject to forces beyond those measured through sensors, no matter how sophisticated, and these forces play roles which are instinctively known but digitally ignored.[35] The target produced from such a system is stripped of its context and is instead constructed from moment to moment from data available to the system. How it arrived in the gaze of the targeting process is unknown and irrelevant. The reason for excluding the unmeasurable and unobservable is twofold, and best understood by conceptualizing the

targeting process as a sociotechnical system. When understood through this lens, targeting assemblages do more than just generate knowledge about the battlefield; they are in fact mechanisms of control.

As also noted by Scott, "Any large social process or event will inevitably be far more complex than the schemata we can devise, prospectively or retrospectively, to map it."[36] In this regard, the United States and allies' brief flirtation in Iraq and Afghanistan with so-called Human Terrain Teams is instructive. These teams were deployed to gather cultural knowledge, complex and qualitative information meant to inform operational choices. In practice, their work was arguably set aside as the conflict became led by remote surveillance and targeting, and less by counterinsurgency practices. The introduction of these unquantifiable insights proved challenging to the established forms of knowledge aggregation prized by the institution, which ultimately reverted back to more familiar and relatively streamlined processes.[37] Whatever knowledge this ultimately excluded may or may not have been crucial to victory. But the primarily datafied representation of an adversary acts as a mirror for our own military organizations, driving decisions about how to fight and with what—revealing the degree of control these preferences exert upon our practices.

Efficiency as an End unto Itself

As discussed above, technology can serve wider, sometimes unseen objectives, acting as a conduit for institutional control every bit as much as a neutral, rational conduit for military victory. This is often obfuscated behind the logic of efficiency, which is located as the driving force of technological development. This phenomenon has for decades been explored by philosophers and economists. Frederick Taylor's *Principles of Scientific Management* introduced the Industrial Revolution to new ways of maximizing productivity through the identification and sequencing of discrete tasks.[38] Martin Heidegger warned that modern technology, rather than serving as an instrument, instead instrumentalizes its users, rendering humans into a "standing-reserve in waiting."[39] Jacques Ellul's notion of *technique*—the optimization of everything to make life uniform, calculable, and ultimately predictable—imparts more value to the artificial than the physical.[40] Michel Foucault examined how technology objectifies its human subjects, stripping them of agency and turning them into "a function, ceaselessly modified."[41] These themes found resonance in the later work of military theorists interrogating the role of technologically-enabled efficiency in war.

technology can serve wider, sometimes unseen objectives, acting as a conduit for institutional control every bit as much as a neutral, rational conduit for military victory.

For instance, Martin Van Creveld juxtaposes *efficiency* (the optimization of time and labor) and efficacy (the ability to achieve a discrete wartime objective).[42] Far from being mutually complementary, these two dynamics in fact work at cross-purposes. Critiquing the Pentagon's rush to introduce electronic mail to every staffer, he highlighted:

> "The original reason for introducing computers into the military, and for linking them to each other, was the amount of information needed to manage modern armed forces and modern warfare. Once computers and the networks linking them were available, however, their very existence led to further huge **increases** in the volume of information to be processed. . . . So it went, in an escalating spiral to which there was no clear logical end. Theoretically the object of the exercise was to attain that kind of perfection of which only technology is capable. In practice, it became increasingly clear that this goal would only be achieved when there was nothing left to perfect at all."[43]

Like "the market," or the thicket of self-reinforcing rules generally referred to as "bureaucracy," the danger of automation and artificial intelligence is less that they become lethal by becoming sentient or deliberately malicious, more that their users become irreversibly beholden to them through a less-than-deliberative path dependency.[44] In an economic context, this might be illustrated by pointing out that the logical extension of maximum efficiency in theory would likely lead to mass unemployment in practice.[45]

For instance, the retail sector's push to save on labor costs and streamline inventory management led them to introduce high-tech self-checkout kiosks. The years-long experiment, however, appears to have failed—what stores saved on hiring cashiers and baggers, they ended up losing on costly IT maintenance, physical upgrades and upkeep, theft, and customer satisfaction. "At the bottom of all the supposed convenience" the new tech may have promised, "you do actually just need a lot of people to operate a store."[46] Thus, the goal of efficiency becomes efficiency itself; it is often not in service of pragmatic organizational objectives but becomes another dogma, to be served because more efficiency is seen as inherently better, but is too often conflated with efficacy. As an objective without end, it becomes the perfect shield for other, less obvious organizational goals—including what economist Dan Davies calls "accountability sinks," which offload human responsibility for outcomes onto technologies or processes.[47] The final section of this piece will bring together these different themes.

Conclusion: Technology and the Limits of Observable Data

The logic of targeting that underpins modern conflict obscures myriad contradictions and dissonant objectives. It is driven by a rational but ultimately unrealistic desire to control chaotic wartime environments, as well as to exert institutional control. These instincts tend to rely on technology to flatten complexity—including human agency and causality among friend and foe, alike—in potentially detrimental ways. Moreover, the technologies employed to manage information economies threaten to propagate entirely new ones, demanding ever more resources in a recursive cycle of innovation.[48] The insatiable demands for optimization

lead militaries to conflate efficiency with proficiency, and to adopt a scientistic view of warfare. Consequently, militaries risk neglecting the physical demands of war in service of ever more granular digital representations. A more critical approach to technology is needed.

Recognizing that a mainstream, institutional and practitioner understanding of the role played by technology in war is shaped by *positivism* highlights the limits of targeting, and the practical dangers of further application of algorithms. A Western engineering-led philosophical approach to targeting does not allow why the enemy fights to be interrogated, only that they do fight, and that they must be constructed as a system of targeting possibilities. As these preferences are built into the technology used to target the enemy, and software becomes increasingly "black-boxed," its origins increasingly difficult to understand. The military-defense domain is investing in and integrating greater numbers of AI-supported tools that aid targeting by increasing the volume of data processed, which increases precision, but at what cost to the intent of a campaign? Discussion on what data enters the algorithm and generates the target is closed. Historic preferences for targeting limit further exploration of its consequences. Presenting targeting as the natural evolution of warfare in its current institutional philosophical context closes dissent. Thus, debate is limited to the practical limits of precision weapons rather than systemic interrogation of targeting itself, despite its role in exerting control over entire military organizations and practices. The gulf between the software representation of the enemy, and the enemy themselves in their battlefield reality, is thus ignored in an endless pursuit of both control and optimization.

The conduct of war has increasingly become a fight with a one-dimensional, digital representation of the enemy, extracted from what it is observed to be doing, primarily through sensor input. As targeting continues to abstract war from battle to bureaucracy, what we understand as the enemy is mediated by technology.[49] This engineering-derived algorithmic representation of our enemy is destined to be ever-present, thus never defeated, so how can we alter the philosophical lens through which the battlefield is understood? This article has highlighted that not only is the targeting process a means to find the enemy, but it also seeks control over both its own organization and the battlefield. Efficiency and control have been conflated with efficacy and become means to their own ends. Is it possible for militaries to recognize and temper their tendency "to fit men into the machinery rather than to fit the machinery into the contours of a human situation"?[50]

02

Digital Technology, Strategic Adaptation, and the Outcomes of Twenty-First Century Armed Conflict

Nate Allen

The Russian war against Ukraine has become the latest poster child for a technology saturated conflict, with the proliferation of GPS-guided munitions and social media posts documenting drones zipping around the battlefield. Yet, as some analysts have recognized, the trench-based, artillery-driven warfare in Ukraine still bears resemblance to European wars of the early twentieth century.[51] If digital technology is truly transforming the nature of armed conflict, why hasn't one side leveraged advances in networked communications, information warfare, cyber power, or digitally driven intelligence, sensing, and targeting to decisively gain an upper hand?

The answers to these questions partly lie in the nature of digital technology itself. Digital technology is not like conventional weapons technologies, such as fighter jets, tanks, or explosives. As other analysts have observed, it is an enabling technology that is more akin to electricity or fuel than any individual weapons system.[52] Most digital technologies, including those employed by militaries, are developed by the private sector for commercial use, making them widely accessible. This accessibility has led to so-called open, constant innovation in their employment.[53]

In a number of armed conflicts, this era of open technological innovation has been characterized by rapid cycles of innovation, adaptation, and readaptation. These innovation-adaptation cycles offer one explanation for why some armed conflicts appear stalemated despite digital technology's ubiquity and proliferation. In Ukraine, for

example, Russia's cyber attacks against the satellite networks Ukrainian forces depended on for communications, command, and control were blunted as Ukraine shifted to other communications technologies.

Similar patterns of adoption and adaptation have occurred in Nigeria, where the Boko Haram insurgency first exploited rising cellular network connectivity and then adapted to the Nigerian government's use of these networks to collect intelligence on the group. It has also been the case in Somalia, where, despite being one of the world's least technology rich theaters, internet and social media spaces have become key arenas of contestation between the insurgent group al-Shabaab and the Somali government and its backers.

In all three conflicts, while the employment of digital technology has precipitated tactical advantages and territorial shifts, cycles of readaptation and response have blunted and even in some cases reversed these advantages. The result is the appearance of prolonged stalemates even as digital technology becomes more widely exploited and used.

The Digital and Ukraine

The role of strategic adaptation in shaping the use of digital technology in the Russia-Ukraine war was evident since Russia launched its full-scale invasion in 2022. At the beginning of its offensive against Ukraine, Russia launched a massive cyber attack against the American satellite company Viasat, which Ukraine's military depended on for communications, command, and control. According to a senior Ukrainian cybersecurity official, the attack resulted in a "huge loss in communications at the very beginning of the war."[54] It marked the opening salvo of a concerted campaign by Russia to degrade the ability of Ukraine to communicate and coordinate its operations on the battlefield.

However, the advancement and ubiquity of communications technology meant that Ukraine in short order found viable alternatives. Ukraine contracted with billionaire Elon Musk to provide Starlink satellite–enabled military communications. These satellites arrived and began to be deployed throughout Ukraine on March 1, 2022, barely a week after the attack against Viasat.[55] Because of the large number of satellites in low earth orbit, they are far harder for Russia to jam and enable Ukraine's military to possess greater communications capabilities than at the start of the war.[56] In fact, the use of Starlink, combined with Ukrainian-developed software platforms such as Diia and Delta, have enabled Ukraine to achieve a level of integration in command, coordination, communications, and control networks that have been long sought by, and are now the envy of, Western militaries.

The role of strategic adaptation in shaping the use of digital technology in the Russia-Ukraine war was evident since Russia launched its full-scale invasion in 2022.

Even without Starlink, it is unclear whether Russian efforts to sabotage Ukraine's digital communications would have succeeded. As the *Economist* notes, Ukraine's large number of internet service providers and the use of electric vehicle batteries as sources of power during blackouts would make a complete loss of connectivity exceptionally difficult to impose.[57] Signal boosters using household materials can extend a mobile phone's range up to 15 kilometers (9 miles) if nearby cell phone towers are destroyed. Even as Starlink was being deployed, Ukraine appeared to have been preparing to use signal boosters and short-wave ham radios to use as "a sort of alternative internet."[58] At the edge of the front, World War I–era wind-up phones are deployed to communicate between trenches to help Ukraine evade Russian electronic warfare capabilities.[59]

At the same time, the conflict remains a stalemate. Some might argue that Starlink and other technology prevented Ukraine from complete capitulation. On the flip side, neither Western support nor Ukraine's digital innovations have enabled a decisive Ukrainian victory. This is partly because of well-documented Russian advantages in manpower and munitions. Yet it is also because Russia, while perhaps not to the extent of Ukraine, has itself taken advantage of ubiquitous digital technology to advance its communications and electronic warfare capabilities. Despite the risks, cell phone usage among Russia's military units is reportedly widespread and is at times used by units who either do not have or cannot afford more secure methods of communication.[60] Commercial off-the-shelf apps, such as AlpineQuest GPS, provide Russian forces with tactical intelligence on Ukrainian equipment and positions.[61] Social media apps like Telegram are used for propaganda purposes and to address logistical needs, while Discord live feeds drone footage to command centers.[62] While Starlink is banned in Russia and internet access is limited on the front, Russian elite formations that can afford Starlink are themselves beginning to deploy it in Ukraine.[63] More recently, they have deployed advanced capabilities to the front that enable them to jam Ukraine's Starlink service.[64]

In short, while the evidence would indicate that Ukraine has won the greater benefit from and moved more rapidly to integrate digital technology into its doctrine, the low costs, ubiquity, and accessibility of digital technologies of all kinds have enabled Russian strategic innovation as well. Both sides exist in an environment with many varieties of digital technologies available to them, with considerations such as cost, bandwidth, levels of risk, use cases, and ease of access all influencing how each digital technology is deployed. In this ecosystem of rapid innovation and ubiquitous technology, an enduring advantage is hard to come by.

Cellular Networks and the Boko Haram Insurgency

The Russia-Ukraine war may be on the bleeding edge of the employment of digital technology for military purposes, but similar patterns have played out elsewhere. For example, the rise of the Lake Chad Basin's Boko Haram insurgency—which began in 2009

and saw violence peak between 2014 and 2015—coincided with the rapid spread of cellular coverage in Nigeria. Between 2004 and 2014, mobile phone penetration increased tenfold, to include close to three quarters of the population.[65]

For the first several years of the insurgency, Boko Haram used Nigeria's cellular networks largely unopposed. The ways in which mobile devices enabled the group were manifold. It used mobile phones to coordinate, plan, and even conduct attacks, making consistent and devasting use of cell phone triggered explosive devices.[66] Researchers Jacob Udo-Udo Jacob and Idorenyin Akpan describe a wide variety of tactics enabled by mobile communications, including activating and coordinating remote units placed close to a target location; coordinating simultaneous so-called dummy raids to distract and overstretch security forces; and, in some cases, attacking phone masts to prevent communities being raided from calling for help from security forces.[67]

The state of Nigeria's efforts to stem the tide of the Boko Haram insurgency by restricting its communications can be traced to early 2011, when the Nigerian Communications Commission (NCC) passed a law that mandated the registration of all the country's mobile phones. This enabled security services to leverage Nigeria's communications networks for intelligence purposes and paid immediate dividends in early 2012, when several key Boko Haram commanders were captured.[68] In 2013, as the insurgency continued to spread, the Nigerian military further escalated its response by initiating a shutdown of all telecommunications networks in the states where the insurgency was most active. The intent, according to a senior military commander, was "to cripple [Boko Haram] in the current campaign because without communication they cannot coordinate and that will put them in disarray."[69] The three-month shutdown reportedly coincided with a significant reduction in the number of Boko Haram attacks and an increase in the number of Boko Haram operatives killed.[70]

However, the insurgency undertook several adaptations that enabled its persistence. In 2012, Boko Haram responded to these setbacks by attacking the infrastructure networks of all four of Nigeria's major telecommunications providers, damaging 150 masts and base stations.[71] These tactics have continued, with the group's main intent being to deny state forces intelligence about its intentions and movements.[72] In addition, Boko Haram took steps to reduce its own reliance on Nigeria's telecom networks. More attacks were coordinated via face-to-face meetings, through satellite phones, or by taking advantage of emerging messaging platforms, such as Skype or WhatsApp.[73] Boko Haram also relocated its headquarters to the Sambisa Forest, where it was less vulnerable.

Today, Boko Haram remains a rural-based insurgency that is a persistent threat to state authority. Just as in Ukraine, even as digital technology has become more ubiquitous in Nigeria, cycles of adaptation and re-adaptation have helped prevent Boko Haram from seriously threatening the state and the state from fully eliminating Boko Haram. In the early stages of the insurgency, Boko Haram appeared to have leveraged novel information and

communication technologies to enable its growth and spread. The state response to assert increasing control over Nigeria's telecommunications sector has limited this spread but has been far from sufficient to end, or even significantly curtail, the insurgency.

The Internet and Al-Shabaab

The pattern of digital strategic adaptation is evident even in theatres where digital technology is relatively limited. Somalia remains one of the world's least connected countries, with an internet penetration rate in early 2024 of just 27 percent of the population.[74]

Nevertheless, the spread of the internet has had a crucial impact on the development of Somalia-based al-Shabaab, which is among Africa's largest and longest-running insurgencies. In the early days of the insurgency, al-Shabaab used the internet to recruit, spread propaganda, and raise a significant amount of money from a vast and supportive Somali diaspora. By 2010, al-Shabaab had its own media foundation that produced high-quality videos, online news and news distribution networks (including local affiliates), radio stations, and social media accounts.[75] Its videos were translated into English, French, Somali, and Swahili, which helped drive recruitment, particularly externally—as many as 1,000 al-Shabaab recruits were non-Somali, as high as one-third of the group's total strength during that time.[76] Al-Shabaab was one of the first Islamist militant groups to be active on Twitter, which it used to devastating effect to record and disseminate propaganda during its 2013 attack against Kenya's Westgate mall.[77]

Yet even as al-Shabaab became known for its digital savvy, its enemies did not sit still. Antiterrorism and sanctions laws made it substantially harder for the group to receive web-based funding from abroad. Major social media platforms, including Facebook and Twitter, began systematically removing al-Shabaab content.[78] And starting in 2011, much of al-Shabaab's leadership was killed in targeted drone strikes, which were likely enabled through the tracking of their mobile device and internet usage. In 2014, al-Shabaab's leader, Ahmed Abdi Godane, was killed in one such strike, hundreds of which were launched over the following decade.[79]

In the early days of the insurgency, al-Shabaab used the internet to recruit, spread propaganda, and raise a significant amount of money from a vast and supportive Somali diaspora.

Like with Boko Haram, while these attacks may have helped blunt the insurgency's momentum, they were far from sufficient to end it. In the intervening years, al-Shabaab has continued to leverage digital technology in ways that have enabled its persistence and survival. Immediately after its leaders were killed, al-Shabaab briefly foreswore the use of the internet in its territory entirely and continues to limit

access; this may be one reason why internet penetration across much of Somalia remains low.[80] Within its territory and disputed areas, al-Shabaab has either contested or completely co-opted telecommunications networks and companies, paying its fighters through e-money transfer services.[81]

Finally, though al-Shabaab's efforts to reestablish official social media accounts have been somewhat suppressed, it has maintained a persistent presence on social media by establishing entities that do not appear to be directly affiliated with it but that often post or link to pro-al-Shabaab content. Shahada News Agency, which is owned by Al-Shabaab, recently announced the launch of accounts on Facebook and X, and its intent "to include coverage of all countries in the Islamic world."[82] A 2022 investigation by the Institute for Strategic Dialogue found the Islamic State and al-Shabaab operating largely unencumbered on Facebook, maintaining thirty public pages with close to 40,000 followers, 445 supportive profiles, and 850 videos garnering 450,000 views.[83]

Despite being the least technology saturated theater, the Al-Shaabab case illustrates a similar dynamic to both Ukraine and Nigeria. Even when a group has been denied access to digital technology completely or concluded that the risk of relying on digital technology outweighed the costs, it has found ways to persist and thrive.

Can't Win With It, Can't Win Without It

In all three conflicts, even as the use of digital technology proliferated, its employment did not lead to a decisive victory for one side over the other. Today's era of open technological innovation, with its rapid innovation and adoption cycles, may help explain why certain conflicts have stalemated. Digital technology's low cost and wide availability give combatants many communication options. Even in cases where one side possesses significantly less-advanced digital capabilities than their adversary, as is the case with Boko Haram and al-Shabaab, it is possible for that side to remain a potent threat.

These cases demonstrate the degree to which accessible digital technology has saturated the world's armed conflicts. Due to this accessibility, strategic adaptation and innovation are continuous. In such a world, the choices about how to employ digital technology, respond to how an adversary employs digital technology, and adapt to constant evolutions in digital technology are paramount. In cases in which both sides have adapted digital technology to suit their doctrine and force structure, victory may not be achieved by digital technology alone.

In other words, in a technology-saturated world, a premium is placed on strategic decisionmaking. This helps explain how some conflicts appear stalemated even as digital technology becomes more integrated into battlefield operations. Like fuel or electricity, it is impossible to wage modern war effectively without digital technology. Yet bombs and brains, not ones and zeros, determine the victor.

03

War and Law in a Digital World

Aurel Sari

Technological advances over the past century have enabled modern armed forces to project power at a scale and speed never seen before. In parallel, the information revolution has dramatically expanded the capacity of ordinary citizens to actively participate in war by producing, relaying, and consuming information. Mediating war has thus become one aspect of fighting it.[84]

These developments call into question whether traditional theories of war are still adequate for understanding contemporary forms of warfare. Some commentators have argued that the information revolution has radically transformed the nature of war by erasing the distinctions between bystander, victim, and perpetrator to create a new hierarchy of war where everyone is now a participant.85 If so, the implications are profound, not least from a legal point of view.

The modern law of armed conflict is built on the principle of distinction—the idea that to avoid unconstrained warfare, lawful targets must be distinguished from civilian persons and objects.86 If the information revolution really has turned civilians into participants in warfare, this may render them lawful targets liable to attack. Should this affect a large number of civilians or even the civilian population as a whole, it could compromise the principle of distinction as the pillar on which much of the law of armed conflict rests. In turn, this could open the door to unlimited warfare.

There is no denying that the information revolution puts the principle of distinction under significant pressure. Even so, the idea that the traditional binaries of military and civilian, participant and bystander, war and peace, have collapsed into one another overstates the case. This piece argues that, at least for now, the key legal challenges lie elsewhere.

Making Sense of Modern War

Classic doctrines of war may go some way to accommodate new developments in the conduct of warfare. For example, Prussian general and military theorist Carl von Clausewitz insisted that the essence of war is combat,[87] yet he also recognized that the intensity of war varies a great deal in actual practice, to the point where it may consist of a mere threat of force without actual hostilities.[88] His understanding of war not only helps to distinguish war from nonwar on a general level but also between different forms of participation in war with reference to whether they involve participation in combat. Some forms of participation may transform a bystander into an active participant, whereas others may not. This is reflected in the law of armed conflict. Civilians enjoy general protection from the dangers of military operations, but they lose this protection and become liable to attack for such time as they take a direct part in hostilities.[89] Using a smartphone to direct an assault against enemy forces without doubt amounts to direct participation in hostilities, but using the same phone to rant against enemy forces on social media or donate funds for the war effort does not. In the eyes of the law, not all digital participation is equal.

In everyday practice, most governments and people are also capable of distinguishing war from nonwar and participation in combat from other forms of supporting the war. For example, Russian missiles and drones have crossed into the territory of nations bordering Ukraine on several occasions since 2022, yet these were not treated as Russian acts of war against the North Atlantic Treaty Organization (NATO).[90] Likewise, there is a very real difference between picking up a Molotov cocktail and hurling it at an advancing tank compared to posting a video of the same event on social media. The digital revolution has not led to the collapse of all existing categories and distinctions. The extremes are still distinct and often can be distinguished from one another without too much trouble. Rather, the problem lies with the many gray cases that fall between the extremes. For example, Western support for Ukraine in its war with Russia raises the question of whether Western nations qualify as cobelligerents. Similarly, a civilian's use of a mobile phone to transmit actionable intelligence poses the question of whether doing so meets the definition of direct participation in hostilities.

The digital revolution has not led to the collapse of all existing categories and distinctions. Rather, the problem lies with the many gray cases that fall between the extremes.

Looking at these matters from a broader perspective, it is also important to bear in mind the normative function of law. It is sometimes claimed that the existing rules are not fit for the conditions of contemporary warfare. Yet the fitness of the law is not simply a question of whether the rules accurately *reflect* the realities of modern war but whether the law is fit for the purpose of *regulating* modern conflict. Law is not a descriptive project but a normative one that holds up the image of a certain future and requires conduct to conform to that image. The point is that if technological developments have led to wider civilian participation in war in a way that disrupts existing legal categories and thresholds, it should not readily be assumed

that the law is out of touch and in need of change. Instead, one should ask whether those categories and thresholds serve valuable goals and, if so, how they might be reinforced to secure compliance. In other words, it should not automatically be assumed that the law must bend to reality, but one should ask whether reality should perhaps bend toward the law.

Is the Law Out of Date?

Even if traditional binaries have not collapsed completely, the divide between active participant in war and passive bystander has become more elusive. This does pose significant legal challenges. Most of the rules and legal concepts that apply in this area were designed for the pre-digital age. Often, it is not clear how they apply in the digital era. A cyber operation carried out by Ukraine's military intelligence services against Russia in 2023 illustrates the point.

According to reports published in December 2023, Ukrainian intelligence services gained access to several central servers of Russia's tax authorities, infected them with malware, and managed to destroy the databases hosted on them and on hundreds of regional servers.[91] As a result, Russia's tax services were said to have been left paralyzed. Since the cyber operation took place within the context of the ongoing international armed conflict between Russia and Ukraine and had a clear and acknowledged nexus to that conflict, the law of armed conflict applies. The main concern from this perspective is whether the Ukrainian operation complied with the principle of distinction, that is the duty to spare civilian objects and persons and direct military operations only against military objectives. The application of the principle hinges on two major questions.[92]

The first question is whether data is an "object" for the purposes of the targeting rules of the law of armed conflict. This matters because the principle of distinction only protects civilian objects: if data is not an object, the principle of distinction does not prevent the destruction of potentially vast quantities of data, including of the type held by Russia's tax authorities. The question is debated in the literature and has not been conclusively answered in state practice.[93]

Assuming that data fits the definition of a civilian object, the second question is whether the destruction of data amounts to an "attack" for the purposes of the law of armed conflict and thus triggers the various rules that must be observed in the conduct of attacks. The notion of an attack refers to an act of violence against an adversary, whether in offense or defense.[94] It is not immediately obvious why deleting data used in the ordinary operation of a computer system—that is in a way that does not cause kinetic harm to the system itself or produce destructive effects—would amount to an act of violence.[95] Deleting data without causing material damage may be described as an act of violence if the notion is extended to acts that do not cause kinetic harm but still prevent a computer from functioning, for example, by corrupting its operating system in a way that renders it inoperable. However, it is not clear whether state practice supports such an understanding of the notion of violence and, in any event, whether the mere deletion of data without compromising a computer's operating system satisfies the requirement.

Legal Narratives and Information Advantage

The digital transformation of warfare poses a long list of technical questions about how the existing rules of war apply to novel developments on the battlefield and beyond. In addition, the information revolution has opened the floodgates for employing law and legal arguments for the purposes of contesting the information environment.

Modern information and communication technologies facilitate the production of legal claims and arguments in a variety of formats, such as simple social media posts and extensive and highly sophisticated blogging. As in other spheres, the ease with which such legal information can be produced, transmitted, and consumed has led to greater participation in these activities. This has given access and a voice to a wide variety of actors from diverse backgrounds and with varying levels of status and expertise, including public officials, private citizens, reputable experts, lay persons, and imposters.

The impacts of these developments are considerable. The greater variety, speed, volume, and diversity in the production, availability, and flow of legal information has made it more difficult for traditional actors, including governments, to deploy effective legal narratives, understood here as the representation of events from a legal perspective.[96] Simply put, traditional actors struggle to tell their legal stories in compelling ways. Government narratives compete with a torrent of other stories, which are produced and deployed at a speed that traditional bureaucracies were not designed to match and at volumes that are difficult to comprehend. Although the quantity of both expert and nonexpert commentary has increased, the inability to process much of the available analysis nonetheless levels the playing field. The sheer number of expert analyses, and the fact that they often point in very different directions, undermines their authority.[97] In fact, not only are expert analyses caught in the crosshairs of social media contestation and tribalization, but the dividing lines between objective scholarly analysis, legal activism, and partisan engagement are not watertight to begin with. In such an environment, legal misinformation, whether borne out of ignorance or deliberate design, spreads easily, and legal narratives are often deployed for information advantage.

Legal commentary on social media platforms is characterized by a rush to reach definite conclusions that typically lack nuance and a sufficient foundation in fact and in law. Much of the debate seems animated by a desire to score points by appealing to legal norms, in particular to legitimize one side and delegitimize the other, rather than an attempt to grapple with what are often complex legal issues arising in circumstances of factual uncertainty. As a result, the law is threatened not only by noncompliance and interpretations that seek to escape some of its constraints but also by overly restrictive interpretations that bear little resemblance to mainstream understandings of the rules and to operational realities. The use of law as an instrument of information warfare may be highly corrosive for the rule of law.

The use of law as an instrument of information warfare may be highly corrosive for the rule of law.

Conclusion

The potential of technological innovations to disrupt the established patterns of war is immense. This is not, of course, a new development: warfare is not static. What is new is the fact that the increased reach, tempo, destructiveness, and availability of conventional force is now married to the ubiquity, speed, scale, and impact of measures short of war, including in the digital and information spheres. This has, among other things, enabled wider participation in hostilities. However, the idea that these developments have fully erased the dividing line between active participants and passive bystanders in war presses the point too far. The line has certainly become more blurred or porous, but at least for now, it is still meaningful to distinguish forms of participation in war that amount to direct participation in hostilities and other types of engagement that are not so closely related to combat. Indeed, this is a line worth preserving in an attempt to prevent a slide toward unconstrained warfare.

Sweeping claims that the regulatory framework of war is out of step with current strategic realities also go too far. Such claims ignore the fact that the law is reasonably well equipped to deal with the disruptive effects of technological change and the transformation of warfare. They also risk diverting attention away from other, more pressing challenges, in particular the lack of agreement as to how specific pre-digital rules apply in an increasingly digitalized battlespace and the way in which modern information and communication technology fuels a contest of competing legal narratives that turns law and legal arguments into an extension of the warfighting effort.

04

Foreign Fighters 2.0: The Interplay of Technology and Lived Experience in the Russia–Ukraine War

Jethro Norman

Introduction

In a café in central Kyiv during the summer of 2023, I witnessed an encounter between two prospective foreign fighters that vividly encapsulated the transformation underway in contemporary warfare. Ramon, a young Spanish technology professional who had never handled a firearm, sat across from Trevor, an African American Iraq and Afghanistan war veteran grappling with PTSD. As they discussed encrypted messaging apps, cybersecurity, and drone warfare tactics, their conversation underscored a profound shift in who is joining modern conflicts and how they engage once they arrive. Historically, foreign fighters have been predominantly defined by prior military experience and ideological zeal; however, the Russia-Ukraine war is attracting and requiring a distinctly different kind of participant—one whose value on the battlefield is increasingly linked to technological proficiency rather than traditional combat skills.

This article investigates how digital technologies are fundamentally reshaping foreign fighter participation in contemporary warfare, based on ethnographic fieldwork conducted in Ukraine between August and September 2023. By closely observing and engaging with fighters like Ramon and Trevor, both in person and through ongoing digital interactions, I argue that the digitalization of warfare is not only attracting foreign fighters with technical expertise rather than conventional combat backgrounds, but also altering the social and

operational dynamics through which both new and traditional fighters engage with conflict environments. These emergent participants, whom I term "foreign fighters 2.0," embody a convergence of civilian technical expertise and military operations, potentially redefining conventional boundaries between combatants and civilians.

At the heart of this transformation is the growing phenomenon of "participative warfare," a form of conflict participation characterized by digital involvement that extends far beyond traditional physical battlefields. While much existing research has examined digital warfare's remote dimensions, such as online propaganda, crowdfunding of military supplies, and cyber operations, comparatively little attention has been devoted to how these digital tools reshape the experiences and identities of those physically entering combat zones.[98] By ethnographically exploring foreign fighters' lives, this article contributes uniquely to our understanding of how digital technologies simultaneously democratize and complicate participation in contemporary warfare.

The implications of this transformation extend beyond academic interest, presenting tangible policy challenges. How should states and international bodies regulate the involvement of civilians whose primary asset is technological rather than military expertise? What are the implications for military recruitment, operational security, and the legal definitions of combatants when digital proficiency becomes as vital as combat readiness? Furthermore, this explorative research illuminates paradoxes inherent in digitally mediated conflicts—such as how increased digital connectivity and surveillance intensify the importance of face-to-face interactions and secure analog spaces for trust-building and authentic communication.

First, I briefly outline key concepts underpinning my analysis, including participative warfare and the persistence of traditional practices amid technological innovation, drawing lightly on David Edgerton's notion of the "shock of the old." Next, I provide detailed case studies of Ramon and Trevor, whose divergent backgrounds and motivations illustrate broader changes in foreign fighter participation. Finally, I analyze the paradoxes of digital warfare uncovered during fieldwork, demonstrating how simultaneous reliance on and suspicion toward digital technologies reshape military interactions and operational practices. Ultimately, fully understanding today's foreign fighters requires recognizing digital and physical realms as inseparable dimensions of contemporary warfare.

Digital War and the Evolution of Foreign Fighter Participation

The rise of digital warfare fundamentally transforms the landscape of contemporary conflict by blurring traditional distinctions between combatants, civilians, and remote participants.[99] Scholars describe this phenomenon as "participative warfare," characterized by digital involvement extending beyond conventional battlefield boundaries.[100] Digital platforms have become essential for narrative construction, information dissemination, and collective mobilization, enabling global civilian engagement through crowdfunding, open-source intelligence gathering, and logistical coordination.[101]

These digital technologies profoundly reshape the profiles of individuals physically traveling to conflict zones. Historically, foreign fighters were often characterized by their military skills or ideological motivations.[102] However, contemporary conflicts such as the war in Ukraine indicate a broadening of this profile. With minimal logistical barriers (often just a smartphone, encrypted messaging apps like Telegram, and a budget airline ticket) foreign fighter participation is now accessible to technically skilled civilians.[103] Ukraine's conflict exemplifies this shift: Thousands of foreign participants are engaging in complex electronic warfare and drone operations, making technical proficiency in cybersecurity and digital systems as critical as traditional combat experience.

With minimal logistical barriers (often just a smartphone, encrypted messaging apps like Telegram, and a budget airline ticket) foreign fighter participation is now accessible to technically skilled civilians

Yet, paradoxically, this increased technological mediation simultaneously heightens the importance of face-to-face interactions and secure analog environments, highlighting a persistent tension between digital and physical dimensions of modern warfare.[104] Understanding this duality is crucial for both academics and policymakers grappling with the evolving nature of combatants and the regulation of civilian participation in warfare.[105]

Methodology

This article draws on ethnographic fieldwork conducted over three weeks in Ukraine between August and September 2023 and in March 2025, supplemented by ongoing digital interactions with participants. Initially focused on humanitarian organizations, the research shifted organically after chance encounters with foreign fighters revealed significant insights into the evolving nature of digital warfare participation.

Primary methods included participant observation and semi-structured interviews with foreign fighters either serving in or attempting to join the International Legion for the Defence of Ukraine (ILDU) and other units. Thanks to my chance encounter with Ramon and Trevor, I was able to follow them as they navigated their way into the ILDU, meeting with other unit members and ethnographically immersing myself into their world. I also conducted sixteen other formal interviews during this period, though the mainstay of my research with the war volunteers was ethnographic. Participants were accessed through chance encounters and snowball sampling, with interactions occurring predominantly in cafés, bars, and informal social gatherings in Kyiv. Ethical considerations were paramount because of the sensitive wartime context; all participants provided informed verbal consent, identities have been anonymized, and identifying operational details are omitted to ensure security.

Data collection emphasized understanding both digital and physical dimensions of participation, capturing how fighters navigated interactions across online platforms and analog spaces. Field notes were recorded daily and interviews audio-recorded where permissible. Supplementary data included analysis of relevant social media and Telegram channels, although the primary analytic focus remained ethnographic, foregrounding participants' lived experiences to illuminate key transformations and paradoxes of digitized warfare.

Foreign Fighter 2.0? Emergent Profiles in Modern Warfare

My first encounter with Ramon and Trevor occurred in a café in central Kyiv during my fieldwork in late 2023. I struck up a conversation with Ramon, and after a pause, he asked expectantly in a soft Spanish accent, "Are you a volunteer too?" The café was largely empty. I assumed he thought I was one of the thousands of informal aid volunteers. I explained my role as a researcher interested in humanitarian organizations in Ukraine and invited him to join me.

Ramon explained that he had just arrived in Ukraine and was now waiting to meet a contact he had met online who would help him get into volunteering. He was a skinny, nerdy-looking guy in his mid-twenties, clearly not ex-military, and his excited, nervous demeanour suggested to me he was a fresh-faced aid worker on his first assignment. Yet something about the way he awkwardly enunciated the word "volunteer" made me do a double-take and question my assumption that he was a humanitarian volunteer. Before I could press further, we were interrupted by the unmistakable arrival of his contact, Trevor.

Trevor brought a very different energy to the table. His frenetic, animated presence filled the space as he immediately launched into sharing his life story. Within minutes, he revealed his background as an Iraq and Afghanistan veteran, his forced medical retirement, and his subsequent struggles with complex PTSD. Only then did I realize that Ramon was not meeting Trevor to make his way into the humanitarian world, but to try to join ILDU. This chance meeting of two ostensibly different war volunteers—a tech professional and a military veteran—would help illuminate the larger transformation happening both on the battlefields of Ukraine and within Western society.

The Tech Specialist

Ramon's skills are an asset in a landscape where traditional warfare intertwines with the digital. Modern combat requires expertise beyond the barrel of a gun; proficiency in cyber systems, drone operations, and communications—areas where Ramon's aptitude shines—is essential.

Ramon exemplifies an emergent archetype in modern warfare: the technically skilled civilian whose expertise has become increasingly vital in contemporary conflicts. As we spoke over several meetings, he revealed his impressive background in electronics, cybersecurity, and

innovative computing at a multinational technology corporation. Despite his youth and lack of military experience, these skills positioned him as a valuable asset on Ukraine's increasingly digitalized battlefield.

Ramon had become drawn to the conflict through the media coverage on social media, especially video footage he watched online. That said, he had grown up in a social environment that was very anti-military. When he was young, he had dreamt of becoming a robotics engineer. He was only in his early twenties, but had already worked in electronics, at a cybersecurity company, and then at a large multinational technology corporation where he won a global award for his innovative work in computing. Now he had taken an indefinite leave of absence from his fast-track career and traveled to Ukraine, initially concealing his true intentions from most friends and family under the guise of "interrailing and doing volunteer work in eastern Europe."

Ramon was naturally humble, but didn't shy away from emphasizing his skills: "I have this good career. I'm really good with computers. I'm really, really good." I didn't doubt him, but if so, I asked, why leave? "The work and consulting is fucking boring. I got burnt out really bad," he explained. Then a friend who had joined ILDU reached out because he was facing problems with his computer, including cybersecurity attacks apparently from Russian hackers. Ramon gave him some pointers on how to protect himself from cyber attacks, and eventually this friend persuaded Ramon to join ILDU as well. Ramon saw in Ukraine the promise of being part of something special and historically significant. He clearly had a moral—even ideological—motivation: "This is a fight against fascism, basically . . . And I truly believe in the European project." Yet the war was also an opportunity. "If I want to make a career for myself later in the defense sector, where can I learn more than here, right now? So I have already some contacts here. I'm trying to get them to teach me how to make kamikaze bombs and things like that."

The Veteran Adapting

Trevor's story stood in sharp contrast to Ramon's. His initial boundless energy at our first café meeting masked a complex narrative of military service, trauma, and a search for renewed purpose. In our conversations, Trevor framed even his civilian life through martial metaphors: "I grew up in a battleground where I was one of, like, two minorities." His path to Ukraine was shaped by profound personal trauma, including the devastating experience of finding his best friend, a fellow veteran, dead by suicide one morning.

As our meetings continued, often extending into late-night conversations, Trevor revealed how the invasion of Ukraine had become an obsession that contributed to the collapse of his marriage. Like Ramon, he had become fixated on the endless reams of footage from the war that reverberated through his social media apps. "I

"This is a fight against fascism, basically . . . And I truly believe in the European project."

"I just felt, like, the calling, and I was like, I want to go. I need to go.

tried to come. I was married at the time. I'm still technically married, but my wife was just like, no! And I kicked off. I was just like, this is it, this is World War Three!" The conflict represented for Trevor not just Ukraine's survival but his own: "I just felt, like, the calling, and I was like, I want to go. I need to go. And it's like, I'm helping out Ukraine, right? But they're helping me out. I have, like, a fucking purpose again."

While Trevor came from a more conventional military background and had combat experience, he was also trained as an engineer and after being discharged became somewhat reclusive yet interested in computers and technology. Like Ramon's, Trevor's journey to Ukraine was thoroughly digitized, facilitated by digital platforms and online communities. Over beers, he showed me his smartphone, scrolling through seemingly endless Telegram messages from prospective recruits. "Look for yourself," he said, "that's just from today." His own recruitment process had involved a complex web of digital connections: initial contact through Reddit forums, verification via Telegram, equipment sponsorship through the "Protect a Volunteer" online charity, and coordination of medical supplies through Polish-Ukrainian online contacts. Now he had become the digital interlocutor, having spoken with Ramon online and finally met him in that café in late August to guide him through the process of joining ILDU.

Paradoxes of Hyperconnected Warfare

As I spent more time with Ramon, Trevor, and their wider group of war volunteers, the paradoxes inherent in their relationship with digital technology became increasingly clear. Despite sophisticated reliance on digital platforms for recruitment, coordination, and operations, volunteers consistently exhibited deep skepticism toward digital communications, fearing surveillance and compromised security. Ramon and Trevor, for instance, quickly dismissed popular apps like WhatsApp and Telegram in favor of Signal—ostensibly a more securely encrypted platform—emphasizing digital vigilance in a highly surveilled environment.

Such concerns are not unfounded. Early in the conflict, Russian forces reportedly targeted a training base after detecting multiple foreign SIM cards clustered together, resulting in significant casualties.[106] This incident underscored the inherent vulnerability of digital technologies, prompting fighters to rely heavily on secure, analog environments for critical communications. I observed as spaces like strip clubs emerged unexpectedly as vital sites for authentic, secure discussions precisely because they enforced strict prohibitions on phones, effectively insulating conversations from digital surveillance. These analog spaces became crucial, offering an unmediated environment for trust-building and sharing unfiltered truths about combat realities.

Beyond mere security precautions, the necessity of physical spaces points to a deeper process of emotional and interpersonal bonding essential to military cohesion. While digital platforms act as gateways facilitating initial recruitment and logistics, the transition from

virtual to physical presence is marked by profound emotional connections formed through face-to-face interaction. In-person camaraderie, often fostered through shared hardships, informal gatherings, and collective experiences, solidifies bonds that digital interactions alone cannot replicate. For instance, foreign fighters sometimes used GoPro action cameras to capture authentic, unfiltered combat experiences, not only for social media and promotional purposes but as a reflection of their deeper need for emotional validation and collective memory shared offline.

These ethnographic insights highlight that despite warfare's technological advancements, the fundamental human experiences of trust, camaraderie, and collective resilience remain deeply rooted in physical, face-to-face interactions. The Ukraine foreign fighters' persistent reliance on analog spaces amid pervasive digital surveillance illustrates what Edgerton termed the "shock of the old"—traditional practices enduring and intensifying alongside technological advancements.[107] Recognizing and managing these paradoxes holds significant policy relevance, particularly concerning operational security, combat effectiveness, and the integration of civilian technical specialists into military contexts.

Conclusion

This examination of foreign fighters in Ukraine underscores a fundamental transformation in the interplay between technology and participation in contemporary warfare. The experiences of Ramon and Trevor illustrate the rising significance of civilian technological expertise alongside traditional combat roles, potentially reshaping recruitment dynamics and operational effectiveness. Yet while digital technologies have facilitated broader and more accessible participation in conflict, they have simultaneously underscored the enduring necessity of face-to-face interactions and secure analog spaces. Trust-building and operational cohesion—critical to effective combat units—depend heavily on sustained physical interactions following initial digital recruitment efforts and are arguably intensified by the hyperconnected state of the battlefield.

While historical analogies to past foreign legions exist, the current scenario in Ukraine distinctively emphasizes how ubiquitous digital technology, such as smartphones and laptops, profoundly impacts the practicalities of recruitment, coordination, and engagement in contemporary conflicts. This research underscores the critical need for policymakers to develop responsive frameworks capable of navigating these hybrid warfare dynamics, balancing technological advancement with the enduring necessity of human interaction and trust.

Finally, while this article focuses ethnographically on Ukraine, many of the dynamics it traces (particularly the integration of civilian tech expertise into conflict zones and the reliance on digital infrastructures) are increasingly visible in other theaters of war, including Somalia and Mali. Indeed, prior to Russia's 2022 invasion of Ukraine, similar patterns were already emerging among foreign fighters and local armed actors in these regions, where digital tools have become both assets and vulnerabilities.[108]

05

Digital Connectivity and Digital Informants in War

Jack McDonald

Digital connectivity is reshaping the latent threat that civilian informants pose to armed forces in war. Smartphones and associated technologies currently enable any civilian to potentially pass verifiable target data to both local and distant forces almost instantaneously. Structurally, this should not be a surprise: technological change often enables new forms of individual or social action in war, sometimes with significant tactical or strategic implications. Some novel technologies therefore force a rethinking and reframing of the way war and warfare are evaluated in normative terms—the assumptions that underpinned previous understandings of right and wrong no longer seem to hold true in the present or near future.

Digital communications technologies, notably smartphones, have empowered civilian informants in conflict zones. Armed forces have historically had to deal with the fact that civilians may function as spies or pass information to opposing armed forces in an ad hoc manner.[109] However, today's civilian observers to armed conflict likely have access to a smartphone that can transmit photos and videos, as well as GPS location data, in a near instantaneous manner.[110] This information can be utilized at a local level, enabling direct strikes upon an opposing force, and at an operational level, enabling one side to better understand the disposition of the other side.

Relatively small acts, such as taking a photo and uploading it to social media channels watched by combatants, can have significant consequences. This is because digital media lends itself to forms of communication that are distinctly more useful than spoken word communication. Today's digital conflict observers can transmit trusted, timely, rich, and precise data that is inherently integrable into force decisions and kill chains.[111] A combatant would not have to trust or rely upon an observer's knowledge of military equipment to verify the model of a photographed armored fighting vehicle. Equally, photographic and video data can provide precise geolocation information that is impossible to capture in spoken communication.

The legal and moral understanding of civilian liability to harm in war is hard to reconcile with the nature of digital observers and informants in contemporary conflict.

As a consequence, digital connectivity has destabilized the concept of participation in war. The legal and moral understanding of civilian liability to harm in war is hard to reconcile with the nature of digital observers and informants in contemporary conflict and the threat that they can pose to combatants. Therefore, it is necessary to explain the problems this creates for armed forces in war and begin to explore areas of policy development and professional training to better equip them to address this issue in future conflicts.

This article highlights the challenges posed by general digital connectivity for states and their armed forces. It frames the issue in terms of how digital connectivity reshapes threats posed by civilian informants and identifies key policy problems, such as managing how armed forces interact with suspected digital informants, and the incentives states create for their citizens to collect information in armed conflicts.

Digital Informants as Empowered Observers

Digital connectivity changes the practicalities of civilian involvement in war. Specifically, smartphones and digital communications platforms increase the ability of civilians to collect data and information relevant to military operations and reduce the barriers to acting as a civilian informant to one (or more) sides in an armed conflict. A recognized key challenge of contemporary armed conflict is that civilians, in near real time, are able to communicate information that can be directly integrated into military targeting processes. This is in contrast to civilians making one-off, informal contributions or passing information that feeds into the planning of broader military operations, rather than specific attacks.[112]

Smartphones draw attention to the myriad forms of informational work that civilians can undertake in the context of war. Although researchers typically focus upon civilian involvement in terms of physical labor, such as firing weapons, civilian labor can also take the form of service provision or the production of intangible goods—observation and intelligence collection, information processing, and communication—that can equally help one side or the other in war. While there is a physical dimension to these roles and acts, their intangible nature makes their connection or contribution to armed conflict difficult to observe and measure.

Here, it is worthwhile to consider that some forms of what might be called information work have traditionally been recognized as significant issues in regulating war. Spying poses a grave threat to armed forces, so civilians found to be engaged in spying were and are liable to be treated extremely harshly if captured. In practical terms, there has always been a trade-off between the utility of punishing spies, collaborators, and informants and the legitimacy challenges associated with punishing them.[113] Children and civilians often keep watch on military bases in expeditionary or counterinsurgency conflicts, and acting against them is

likely counterproductive. In these kinds of conflicts, enraging a local population by detaining children suspected of being informants is unlikely to be worth the effort. International humanitarian law provides special and specific protection for children in armed conflict, which reflects general social intuitions that using force against them is qualitatively different from attacking adults.[114]

It is necessary, however, to distinguish between intelligence officers (spies) and their agents who feed them information or undertake actions at their behest. This second category might further be subdivided into collaborators—those who systematically work for, and collect information on behalf of, security forces—and informants—those who might provide information on an ad hoc basis.[115] The reason for making such a distinction is that while both collaborators and informants have been prevalent in wars past and present, digital connectivity has empowered informants and increased the threat that they pose relative to intelligence officers and established networks of agents and collaborators.

The ability of average citizens to act as sources of timely, trusted, rich, and precise data is a consequence of digital connectivity. Equally important is that the barriers for individuals to engage with armed forces in war—in other words, moving from neutral civilians to civilian informants or collaborators—have also been greatly reduced by the same set of technologies. As a result, armed forces find themselves operating in an environment where the threat that civilian informants pose has been greatly increased, their opponents find it easier to trust the information provided by civilian informants, and it is far easier for any civilian with a smartphone to become a civilian informant.

Digital Participation in War

By empowering observers and civilian informants, digital connectivity is changing the practicalities of participating in war. The various uses of digital communications technologies by civilians have focused attention on the extent to which they alter civilian participation in war and, relatedly, the extent to which civilians are then liable to attack or cause harm.[116] This is typically discussed in terms of distinguishing between indirect participation—acts and activities that civilians cannot be attacked or punished for committing—and direct participation—acts and activities that cause them to lose the protection of civilian status for some length of time.[117]

The problem of digital participation in war is compounded by the fact that the regulation of war primarily focuses on physical threats and harms. Information processing, and forms of work associated with the processing and communication of information (or intelligence) are lightly regulated in relative terms by the law of armed conflict and have only recently begun to be seriously studied in terms of just war theory.[118] Whereas considerable effort has been expended considering the extent to which physical acts and labor roles might cause a civilian to be liable to attack,[119] less effort has been put into understanding intangible acts and activities, such as information communication and processing, despite their growing prevalence in contemporary warfare.

Intangible contributions to acts of violence have been recognized in some recent debates about international law. This was first notable in complicated debates about the relationship between cyber attacks and war, but the very nature of these contributions makes them harder to classify and categorize.[120] Many of the topics of analysis and points of debate regarding civilian participation in war are focused upon physical acts or roles requiring physical labor. In this sense, there is a notable bias toward analyzing civilian participation in war via physical work or exertion. When considering digital civilian informants, we must think beyond intangible methods of attack or disruption and instead consider how the traditional foregrounding of physical contributions to war limits our understanding of developing modes of intangible contributions to war that may enable larger scale harms than individual acts of violence.

Digital connectivity has expanded the range of ways in which civilians can observe and understand war, as well as forms of information work that can directly contribute to physical acts of harm. Considering what civilians can achieve in terms of information processing, it is hard to distinguish some forms of direct participation (such as providing data for targeting purposes) from the actions of civilians that normally would not be considered legitimate military targets. For example, if someone were to geolocate a military object from open data, publish this geolocation online, and this information was then used by combatants to target the military object, the main effort of the individual's work—geolocation—would be no different to someone who undertook the same analysis but instead directly passed that information to combatants in the armed conflict.

Divergent Thresholds of Harm

The key challenge arising from digital participation in war is distinguishing between forms of digital participation that make an individual or organization liable to attack and harm and those that do not. The potentially outsized importance of otherwise minor actions, such as sharing a photo or a location tag, means that there is a growing tension between the latent threat that civilians pose to armed forces and the regulations that protect civilians in times of war. Civilians might once have aided armed forces by communicating information, but that information would not have much effect on a battlefield in the nineteenth century due to the nature of combat in that period. Conversely, forces operating in contemporary conflicts should now be keenly aware that any civilian with a smartphone could be communicating their exact position in real time to opposing forces.

An October 2023 International Committee of the Red Cross (ICRC) report recognized that digital participation can amount to direct participation in hostilities, therefore resulting in the loss of civilian protection.[121] In addition, some legal scholars have noted that "civilian volunteers involved [in passing information to combatants] lose the essential protections against attacks and their effects that they would otherwise enjoy."[122] There are, however, two divergent approaches to the potential consequences of digital participation.

The first approach, which is taken by the ICRC and the wider humanitarian community, restates existing obligations to prevent civilian harm but also interprets the grounds on which a digital observer might be liable to harm in the most restrictive way possible.[123] At extremes, this can take the form of arguing that a civilian uploading targeting information to an opposing force is liable to be attacked only when that information is directly used for an attack and, even then, only during the second or so that it takes to send the information. This approach, while it might make sense in theoretical terms, perhaps ignores the fact that it is entirely impracticable in the real world. Given that combatants would not know the exact sequencing of information processing by their opponents (whether the information is used directly or processed in some form to create an intelligence product that might also adversely affect them), nor would they realistically be able to time an attack for a button press, the restrictive interpretation of digital participation effectively insulates civilians from attack, even if they are directly aiding attacks in an armed conflict.

Digital connectivity poses a problem for states seeking to wage war effectively while also minimizing civilian harm.

A second approach that includes a more expansive interpretation of liability to attack is equally troubling. If civilians acting as direct observers might be targetable, what about civilians performing tasks like geolocation on open-source data? Geolocation can produce intelligence products that are even more useful for the purposes of an attack than the location of a single tank. Open-source intelligence (OSINT) researchers regularly study the location of strategic facilities, such as those associated with North Korea's nuclear program, and can geolocate operational targets such as military bases. In this regard, the potential expansion of liability to attack and harm implied by civilian uses of digital technologies is enormous.

Consequently, digital connectivity poses a problem for states seeking to wage war effectively while also minimizing civilian harm. One way of understanding digital connectivity's effects is that it has reduced the scope for optimum policy and practice that balances the risks to civilian populations against the security of armed forces in the field. States can make policy choices on who, or what, they consider to be liable to harm for information collection and processing in war, but on a theoretical level it is hard to justify a principle that reasonably includes digital informants without over-including a huge range of civilians with access to the internet. This problem is likely to become even more salient as such distinctions are coded into artificial intelligence (AI) systems used to distinguish and identify targets in contemporary and future wars.[124]

The Need for Policy Responses

How should states respond to the challenge digital informants pose to society's understanding of participation and restraint in war? This section highlights two key areas where states may need to work on developing policy responses to digital informants. The primary

problem is the interaction of armed forces with civilian populations. Since digital connectivity means civilians can enable ambushes and indirect fire, or provide live tracking information on forces, it greatly increases the latent threat that informants pose to armed forces.

The first policy area that needs consideration is how to manage armed forces' responses to digital informants in this new environment given that they have been trained to treat the civilian population as bystanders. Notwithstanding criminal responses (for instance, shooting at civilians indiscriminately or arbitrarily executing civilians found to be passing information to opposing forces),[125] digital connectivity has raised the latent threat that individual civilians pose to soldiers; they must now operate in an environment where any civilian's smartphone could be helping someone target them for attack.

Without an appropriate organizational response in terms of developing standards and procedures, as well as training for such situations, individual combatants are likely to respond in an ad hoc manner. This means that an armed force risks losing control of its own personnel in these situations or seeing varied regimes of interaction between its forces and civilian populations depending upon units and locations. It is therefore necessary to think how an armed force might develop policy and training to standardize, as much as is possible, the way its troops respond to these kinds of situations.

A second policy area is the way in which states collect information from civilian populations during armed conflict and the extent to which that undermines the ability of their civilians to remain neutral (or, at best, indirect participants). As outlined above, there is a need to consider the intangible contributions to war in terms of direct participation and the novel dimension of publishing and communicating information relevant to targeting in war. For states, this adds to the complexities of ensuring civilian protection during armed conflict, an area that already lacks universal interpretations.[126]

In the Russian war against Ukraine, for example, the Ukrainian government has integrated tools for reporting Russian forces into its generalized government digital services platform.[127] The central dilemma here is that states gain an obvious advantage from integrating civilian-produced data into intelligence systems, but doing so makes it hard for civilians to remain neutral. What this points to is the need to evaluate the design of communication systems and digital platforms in ethical terms. For example, if a government makes an app that enables civilians to pass information to its armed forces, use of that app might be considered relevant when determining an individual's connection to armed conflict. Equally, if a government integrates reporting mechanisms into general digital services, to the extent that citizens are unable to access other government digital services without also having access to a reporting function, this makes it difficult for civilians to stay neutral in armed conflict.

Without an appropriate organizational response in terms of developing standards and procedures, as well as training for such situations, individual combatants are likely to respond in an ad hoc manner.

The value of this approach is that it enables academics to conceptualize the stakes for preserving civilian neutrality in digital services and platforms. This, in turn, may help governments negotiate agreements on how to design government digital services in a way that enables the preservation of civilian neutrality in the twenty-first century.

Conclusion

The past twenty-five years have seen overlapping waves of digital connectivity—the internet, then platforms, and then smartphones—spread throughout the world, including into every conflict zone in some form or another. This trend necessitates a rethinking of how intangible contributions to armed conflict may render civilians liable to attack or increase the likelihood of armed forces committing war crimes in response to digital informants.

The two policy areas highlighted in this article—addressing the way armed forces are trained to deal with digital informants, and evaluating the incentives states create for their citizens to become digital informants in armed conflicts—are the most salient of the issues associated with this topic. In the future, it is unlikely that a perfect solution or set of standards will develop in response to these issues, but states should focus on these issues now before divergent responses create problems in coalition warfighting or peacekeeping operations.

06

Participatory War and Its Challenges for Total Defense

Kristin Ljungkvist

Sweden is in the process of not only rebuilding its military capabilities but also reestablishing its Cold War–era, whole-of-society strategy known as total defense. This strategy, deeply embedded in Swedish security policy, is rooted in the active participation of civilians—making broad societal engagement a long-standing national tradition. In Sweden, total defense entails the mobilization of the entire population and legally mandates citizen participation in the defense of the country. Total defense as a strategy historically emerged in response to the threat of total war—a form of conflict that indiscriminately affects all aspects of society and targets not only military forces but also civilians.[128] In such a context, the civilian population becomes both a primary target and a central pillar of deterrence. A robust total defense therefore requires a deeply rooted people's defense: a citizen army supported by widespread public readiness and a strong will to resist.

As Sweden reestablishes its total defense posture today, one of the most significant differences from the Cold War era is the contemporary context of hyperconnectivity. The ubiquity of digital networks and smart devices introduces new dimensions to citizen involvement in conflicts, enabling a more technologically integrated and participatory form of total defense.[129] However, while digitally enabled participatory warfare offers unprecedented opportunities, it also raises questions about civilian protection, trust in public institutions, and the upholding of democratic principles. As governments promote digital civic engagement in defense, they must acknowledge some difficult truths, including the potential deterioration of civil liberties, the unpredictability of digitally mobilized populations, and the legal vulnerability of civilians acting as potential combatants.

Renewed Western Interest in Total Defense

While total defense has traditionally been associated with small, often nonaligned states, recent years have seen growing interest in the concept across Europe and North America. Russia's use of hybrid warfare against Ukraine has underscored the importance of adopting a whole-of-society approach to defense.[130] For example, following the annexation of Crimea in 2014, the European Union (EU) and the North Atlantic Treaty Organization (NATO) launched a joint resilience strategy to counter hybrid threats.[131] Russia's full-scale invasion of Ukraine in 2022 has further prompted a broader reassessment of national defense strategies in Western states.

As the European Council on Foreign Relations has noted, European countries may draw valuable lessons from Ukraine's ability to mobilize a comprehensive response that integrates both military and civilian components, involving actors both within and beyond formal state structures.[132] Ukraine's model has been described as "an innovative and unconventional approach to warfare and total defense that has guided not just Ukraine's military, but also involved the country's civilian population as part of a concerted resistance against Russia's army."[133] As such, it is increasingly being regarded as a potential reference point for adapting defense frameworks across Europe.[134]

The digital domain has emerged as a key battlefield—one in which the general population has engaged in innovative and direct ways.

While characterized by conventional military operations, the war in Ukraine has, since 2014, also been deeply shaped by cyber and information warfare. The digital domain has emerged as a key battlefield—one in which the general population has engaged in innovative and direct ways. Some have described the war in Ukraine as the first inter-state conflict to unfold fully within a context of hyperconnectivity.[135] Digital platforms and social media have significantly expanded the ability of private individuals to disseminate information—and disinformation—thereby enabling civilian participation in the informational dimensions of warfare. Civilian digital devices have become tools not only for communication but also for mobilization, surveillance, and intelligence gathering.[136] In many respects, this form of participatory warfare exemplifies the principles of total defense, in which the boundaries between military and civilian roles are increasingly blurred.

The Implications of Participatory War for Sweden

As Sweden reestablishes its total defense framework, one of the most notable departures from the old Cold War model is the advent of hyperconnectivity. In this context, participatory war has become central to contemporary approaches to total defense. Participatory war extends beyond formal military institutions, relying instead on the active digital engagement of civilians across society. The proliferation of digital networks and smart devices introduces

both new vulnerabilities and transformative opportunities. These technologies facilitate a more dynamic and participatory form of total defense, enabling citizens to contribute in real time to surveillance, threat detection, crisis communication, and efforts to build collective resilience.

During the Cold War, Sweden's total defense legal framework was premised on the logic that active civilian resistance would only be triggered in the event of an imminent or actual armed attack. This was itself contingent upon a government-declared heightened state of alert. In peacetime, under so-called normal legal conditions, total defense primarily concerned war preparedness. However, the strategic logic guiding the contemporary reestablishment of Sweden's total defense reflects a shift: it now centers on the notion of an ongoing hybrid war.[137] Since deciding in 2015 to rebuild the country's total defense capabilities, the Swedish government has repeatedly asserted that the country is subject to daily hybrid attacks, such as cyber attacks, infrastructure sabotage, and disinformation campaigns.[138] In this context, as Matthew Ford and Andrew Hoskins argue in *Radical War*, every individual with a smartphone becomes a potential participant in this hybrid digital war ecology.[139] Framed this way, contemporary Swedish total defense must operate continuously, defending against persistent digital threats to everyday life. The implication is that the Swedish government must prepare its citizens to be capable of actively participating in the digital total defense of the country. This possibility, however, introduces new challenges and responsibilities that reshape Swedish civil-military relationships in three important ways.

First, a constantly activated total defense places new and far-reaching demands on the general population. In Sweden, citizens have become targets of disinformation campaigns designed to polarize and destabilize society. During the Cold War, countering propaganda and ensuring the delivery of accurate information was a state-managed responsibility. However, in today's hyperconnected environment, this responsibility has, by necessity, been decentralized to the individual. As it rebuilds Sweden's total defense, the government has repeatedly emphasized the responsibility of each citizen to resist and mitigate false information.[140] This shift presumes a highly knowledgeable and vigilant population—individuals who are prepared to defend against hybrid attacks, even through seemingly mundane activities such as scrolling through social media. Consequently, building an effective total defense in the age of hyperconnectivity requires an educational system capable of fostering media literacy and critical thinking across the population.

Second, and closely related to this, if every citizen is a so-called smartphone soldier, how can discipline be maintained among the ranks? The unprecedented role of civilians in digital warfare introduces risks of volatility. A central aim of hybrid attacks—particularly through disruptive communication—is to fracture social cohesion, foster distrust, and diminish the public's willingness to defend. In Sweden, willingness to defend is understood to be deeply intertwined with social trust and confidence in public institutions. As such, managing fear and anxiety within the population becomes a national security concern. This logic was visible during the COVID-19 pandemic, when critics of Sweden's public health strategy were frequently accused of undermining public trust and, by extension, of threatening national

security. Some were even branded as spreading false propaganda or acting as security risks.[141] In this context, what might have otherwise been viewed as legitimate democratic debate risked being framed as a threat to national security.

This dynamic echoes concerns raised by David Alexander, who warns that civil defense efforts can be co-opted into instruments of state repression.[142] He notes that "plans to manage civilian populations can turn into strategies for ensuring that protests are repressed or revolts are subdued, even when these are stimulated by a desire to defend or restore democratic rights."[143] While freedom of speech and the right to critique public policy are fundamental to democratic societies, these principles may come under pressure in the context of an approach to total defense that has to adapt to the challenges of hyperconnectivity and participatory warfare. In such environments, dissenting voices and public debate risk being reframed as threats to national security. This presents a profound democratic challenge: in building an everyday total defense, governments must carefully balance the need to uphold civil liberties with the imperative to monitor and counter harmful narratives. Resilient societies will require not only high levels of public trust in institutions but also a broad societal acceptance of the disruptions that hybrid attacks may cause. Striking this balance is essential to ensuring that efforts to defend democracy do not inadvertently undermine its core values.

Third, if conflict escalates into kinetic warfare, hyperconnectivity enables the general population to participate directly in the conflict in unprecedented ways—through digital devices. Citizens may engage in crowdsourcing efforts to support military logistics, share real-time intelligence, or even contribute to targeting decisions. The war in Ukraine has vividly illustrated this phenomenon: private individuals have geolocated Russian forces and transmitted the data to the Ukrainian Armed Forces via government-supported apps, thereby becoming directly involved in the kill chain.[144] Within the strategic logic of total defense, such active and innovative civilian participation is not only welcomed but increasingly expected.

However, this development raises a critical and often neglected issue: by engaging in these activities, civilians may forfeit their protected status under international humanitarian law and become legitimate targets of war, an issue examined by other authors in this Carnegie series, including Aurel Sari's piece "War and Law in a Digital World" and Jack McDonald's article, "Digital Connectivity and Digital Informants in War."[145] In the Ukraine context, the fundamental question of who qualifies as a combatant has received insufficient attention.[146] Governments that pursue total defense strategies in this context must seriously confront the implications of encouraging civilians to engage in digital warfare.

When smartphones become tools for warfare, their users may be reclassified as combatants, at least temporarily.

Indeed, there have been reports of Russian soldiers shooting Ukrainian civilians for simply using their smartphones[147]—actions that may, disturbingly, align with the laws of armed conflict. When smartphones become tools for warfare, their users may be reclassified as combatants, at least temporarily. As Pontus Winther and Per-Erik Nilsson argue, any private citizen who geolocates enemy forces and relays that information to national armed forces likely loses civilian protection for the duration of that act.[148]

At a minimum, governments must ensure that citizens are clearly informed of these legal and ethical risks. Participation in digital war must be based on free, conscious, and informed decisions—not assumed as a patriotic duty. In building a participatory total defense, the responsibility lies with the state to communicate the potential consequences of such engagement and ensure that enthusiasm for digital innovation does not obscure the human costs of blurred civilian-combatant boundaries.

Conclusion

The reemergence of total defense in Western security thinking—catalyzed by the war in Ukraine and the proliferation of hybrid threats—marks a profound transformation in how states conceptualize and operationalize national security. Sweden's revival of its Cold War-era total defense model reflects both a return to whole-of-society preparedness and an adaptation to the contemporary realities of hyperconnectivity and hybrid warfare. In this new strategic environment, the boundaries between war and peace, military and civilian, are increasingly blurred. Citizens are no longer mere observers or supporters of national defense but are being positioned as active participants. They are expected to detect disinformation, contribute to situational awareness, and even assist in targeting during kinetic conflict.

However, digitally enabled participatory warfare brings with it significant risks and democratic dilemmas. The decentralization of responsibilities to individuals not only demands widespread media literacy and resilience but also raises questions about civilian protection, trust in public institutions, and the preservation of democratic debate. As governments encourage civic engagement in the digital dimensions of defense, they must also confront the uncomfortable realities this entails.

Ultimately, building a resilient and legitimate total defense requires more than technological innovation and mass mobilization. It demands a renewed civil-military contract—one that clearly defines the rights and responsibilities of citizens, safeguards democratic principles, and fosters informed, voluntary participation in defense efforts. Without such safeguards, the promise of digital mobilization during times of total defense risks becoming its greatest liability.

07

Digital Communication as a Weapon: The Case of Mali

Mirjam de Bruijn

Digital communication is changing patterns of citizen participation in armed conflicts. It is often credited with democratizing political processes, making politics more accessible to a broader population. In the context of war, however, access to connected devices and social media also makes it possible for people to amplify and perpetuate ongoing violence.[149]

Researchers are increasingly examining the role that digital technology plays in modern warfare. In what Matthew Ford and Andrew Hoskins call "radical war," the capacity to produce, publish, and consume media from one device has collapsed the distinctions between different forms of participating in and perceiving war.[150] Today, everyone with a smartphone can transmit and consume images of war independently of traditional print and broadcast media. In societies affected by war and conflict, these digital representations can additionally serve to justify and normalize further violence. Johan Galtung refers to this as "cultural violence"—the use of words, images, and narratives to legitimize or obscure direct and structural violence.[151] Information shared digitally can shape public perception, reinforce divisions, and deepen polarization, making the act of communication itself a potential vehicle for harm.

This article examines the role of digital communication networks in contributing to cultural violence within the ongoing war in Mali, based on results from several research projects conducted in Mali and the Sahel.[152] It explores different dimensions of the digital landscape within the war, including social media platforms, cross-regional and transnational digital networks, internet and social media shutdowns, and digital propaganda. Digital connectivity has permeated the conflict, enabling Malians to both mitigate and stoke the violence. While digital platforms can provide valuable sites for mutual support and organizing, platforms that rapidly connect large audiences to spread polarized messaging and produce information silos can also heighten and reinforce violent discourse.

Social Media and Digital War

In 2012, a rebellion in Mali's north triggered violent conflict that spread across the whole country and continues to this day. These insurgent forces, espousing a mix of Islamist, ethnic, nationalist, and traditionalist ideologies, are drawn from various segments of Malian society, including the national army. The UN mission in Mali, the French military, and more recently Russia's Wagner Group also have played important roles in the conflict.[153]

These political developments have unfolded as digital communication has expanded from urban areas to the rural countryside and from northern to central Mali. As the war has progressed, the regions affected by the conflict have become increasingly interconnected, both internally and with the outside world. National statistics for Mali show that access to mobile phone communication has risen dramatically; by 2023, 100 percent of the population at least had access to 2G connectivity. The share of individuals using the internet showed similar movement, increasing from 2.8 percent in 2012 to 35 percent by the start of 2024, largely via mobile phones.[154] By the beginning of 2025, almost 20 percent of Malians over eighteen years old were regularly accessing social media platforms.[155] As a result, the country's growing connectivity has transformed patterns of warfare.

Social media is a primary site of communication and connection for Malians. But each platform operates differently, leading Malians to make use of them in distinctive ways. My research teams examined different social media platforms and combined ethnographic research with computational methods, social media analysis, and natural language processing to analyze their uses in the context of Mali's war.

We started social media analysis, combining computational analysis and ethnography on the social media platform Twitter (now X) in 2021.[156] Within Mali, X was primarily used by urban, highly educated individuals. Our findings suggest that X served primarily as a platform for disseminating conflict-related news and facts rather than a place for active discussions about the war's dynamics and stakes.[157] In contrast, our research on Facebook revealed a higher level of debate about the conflict among communities in the Sahel. In some cases, these discussions contributed to polarization and even incited calls for violence.[158]

The audiences also varied across the social media sites. Among the platforms we analyzed, WhatsApp stood out as the most actively used tool for one-to-many broadcasts across war-torn regions.[159] One of its important features was the audio function, enabling access for illiterate individuals. WhatsApp also served as a vital communication tool for many Malians living in conflict zones, who used it to share information, discuss the war, and maintain a sense of community. Since the onset of the conflict, the number of ethnically organized WhatsApp groups has surged. One interviewee based in Bamako explained that he belonged to over forty such groups, most uniting members of his community.[160] These channels served not only to circulate real-time information about battlefield developments but also to reinforce ethnic identities. Many messages focused on historical grievances, cultural pride,

and religious distinctions—constructing a shared narrative in which ethnic identity was reinforced and ethnic oppositions and ethnic violence were perceived as the conflict's core, accusing the state and armed groups of the orchestration of such violence.

As a result, these WhatsApp groups often functioned as ethnically defined communication bubbles, deepening social and political polarization. The narratives exchanged in these digital spaces could have real-world consequences—sometimes acting as sites of cultural violence that justified and fueled retaliatory violence by ethnically aligned militias. In this way, private digital communication becomes part of the machinery of conflict.[161]

Importantly, each of these three platforms—WhatsApp, Facebook, and X—were not isolated from one another. Users often participated across all three, with messages and content circulating between them.[162] Posts on X and Facebook would frequently find their way into WhatsApp groups, further blurring the lines between platforms. Since August 2023, TikTok also gained a prominent place in Mali's mediascape. Its fast-paced, video-driven format has proven especially popular among young people, who are drawn to its mix of dance, music, and short-form messaging.[163]

Overall, social media has become a critical space for the circulation of facts and narratives about the war in Mali. Some uses are productive, such as for sharing facts and updates about the conflict to keep Malians informed and prepared. Other uses, however, legitimize the conflict, offering people reasons to be angry and view their opponents as fundamentally wrong—often through selective interpretations of history.[164] Some platforms function as sites of interpersonal conflict, where individuals from differing sides clash over their beliefs. Others more often operate as sites to broadcast messages to a wider audience of like-minded individuals, spreading and exacerbating polarized narratives.

Networked Participation in War

The advent of wireless communication technologies has also significantly transformed how cross-regional and transnational networks operate in Mali, allowing people to remain connected despite their physical displacement in wartime. The number of displaced people in Mali continues to rise daily as individuals flee violence in their home regions. Many seek refuge in self-established camps around Bamako, the capital of Mali, while others resettle in rural areas in the south or cross borders into neighboring countries, such as Burkina Faso and Mauritania. Mobility in the Sahel is not a new phenomenon; it has long been shaped by factors including fluctuating rainfall, labor migration, and recurring conflict. Sahelian societies are inherently networked, with social and familial ties extending across wide geographic areas, including other parts of Africa, Europe, and the United States. But the ongoing conflict in Mali has heightened this dynamic and made digital connectivity even more important.

Social media has become a critical space for the circulation of facts and narratives about the war in Mali.

Since the onset of the conflict, war-related displaced individuals have played a key role in the formation of networks, primarily communicating through phone calls and WhatsApp groups. The connections between refugees, displaced people, those in war zones, and the diaspora have created a space where the realities of war—including its violence—are constantly shared. These networks provide daily updates on the whereabouts and well-being of family and friends, reporting on militia activities, food shortages, and the deaths of loved ones because of inadequate healthcare.[165]

This form of popular, networked participation in war is extensive, forming a transnational community through which the local atrocities in Mali become shared experiences for a large and dispersed group. Such digital engagement, for some, may also translate into action. This includes sending financial support to displaced individuals as well as more fraught manifestations, such as individuals indirectly continuing the conflict by providing material support for militia members, enabling them to purchase weapons.[166]

In this way, digital networks of dispersed Malians influence the battlefield in direct and tangible ways. As Ford and Hoskins describe, this collapsing of the boundary between the digital and the material reality of the conflict is a core element of radical war. These networks of Malians from both within and outside of Mali are shaped by the flow of information that connects them, drawing them into the war as participants.

Absence of Communication

In a conflict as intrinsically shaped by digital connectivity as the ongoing war in Mali, denying populations online access can become an important tool of warfighting.[167] Fighting that consumed the small town of Boni represents one such example. Boni lies in central Mali, situated in a vast rural savannah area that has been under the control of an armed jihadist group, Kaatiba Macina, since 2017. A few hundred meters from the town lies an army military camp. The Malian army considers the region to be a base for jihadist groups. Kaatiba Macina's ranks are mainly filled with local residents; it is part of a broader coalition of jihadist groups known as Jama'a Nusrat ul-Islam wa al-Muslimin (JNIM).[168]

Boni was a victim of the militants' strategy to cut off cities from the outside world. During three separate periods, jihadist groups blocked roads and prevented the movement of people and goods in response to intensified Malian army operations in the area. The first blockade took place from May to August 2021, the second from February 2022 to August 2022, and the third from August 2023 to March 2025.[169]

The physical blockades were reinforced by digital disconnections instigated by both sides. During the first siege, the government responded by reportedly shutting down Malitel—the state-owned telecommunications provider. Orange, the French telecom, stayed active but only by negotiating with armed groups and likely paying for protection. Over time, relations soured, and in 2023, jihadists destroyed Orange's communication mast. Subsequently,

the Malian government ordered a complete internet shutdown in Boni, hoping to disrupt jihadist communications. But the armed groups had their own secure channels, possibly satellite-based, and were unaffected. Civilians, however, were cut off entirely; they were unable to call, message on WhatsApp, or access the internet for months at a time. A partial digital lifeline returned in the summer of 2024, when Starlink satellites began providing service, but access remained limited to those who could afford it, and neither Malitel nor Orange has returned as of this writing.

The blockades were disastrous for Boni. With no one able to enter or leave the city—and with Boni already overwhelmed by displaced populations—the local market collapsed, and people were confronted with famine. Periods of silence and disconnection obscured the suffering caused by the blockade. Citizens were only sporadically able to reach the outside world through digital connections or via those who physically evacuated the area. The Malian government may have hoped that such isolation would turn residents against the jihadist groups controlling the area. However, the blockades may have had the opposite effect, driving people to seek protection with the jihadists, despite the violence the militants were inflicting.

While communications were disrupted, people still collected digital representations of their suffering, notwithstanding the risks. This footage now shapes the memories and narratives of Boni's citizens who share their experiences in community-based WhatsApp groups and other (closed) digital networks across Malian society. The nature of modern digital technology means that representations of suffering endure long after they occur and can be shared even when they take place in closed-off spaces behind digital blockades. The digital evidence from Boni residents continues to play a dual role in the war: highlighting civilian suffering while also fueling cultural violence by becoming polarized symbols that justify continued fighting.

Propaganda and Polarization

Both the Malian army and jihadist groups are not just trying to control information by shutting down the internet—they are actively using digital tools to spread their own messages and win supporters. DIRPA, the communication department of the Malian army, has played a key role in shaping the war's narrative, and disinformation is an essential part of the strategy. On public platforms like TikTok and X, DIRPA's strategy has proven effective in convincing the majority of the population about the Malian army's strength and progress.[170] Videos featuring women dancing in military attire while praising the army have garnered many likes and shares.[171] However, in more

Both the Malian army and jihadist groups are not just trying to control information by shutting down the internet—they are actively using digital tools to spread their own messages and win supporters.

private digital spaces—such as WhatsApp groups and certain Facebook pages—skepticism about this propaganda is evident. These encrypted platforms provide a safe space for people to express their doubts and discuss alternative perspectives.

This skepticism has also been compounded by online jihadist communications. JNIM's media production company, Al-Zallaqa, disseminates news and messages about its victories and offers select interpretations about its attacks that are then shared on channels reserved for jihadist messaging, such as on Telegram. From there, the information migrates to other social media platforms, such as WhatsApp. During Muslim holidays, these channels disseminate carefully curated images of armed fighters gathered in remote locations sharing communal meals and prayers. This imagery is designed to showcase jihadist unity and attract recruits to their movement.[172]

Broader Implications

This article has outlined how digital telecommunications networks are shaping patterns of violence in Mali. One-to-many digital communication platforms have the capacity to connect large audiences quickly and at scale—far beyond what one-to-one communication tools can achieve. This dynamic has significant implications not only within Mali but across international borders, particularly among the Malian diaspora. In many cases, digital connection provides an important tool for civilians to negotiate the complexities and harms of war, providing sites for information sharing, mutual aid, and connection across forcefully dispersed communities. At the same time, social media platforms and digital tools can legitimize violence, or they can become tools within the warfighting effort itself.

As discussed, platforms such as WhatsApp tend to foster closed communication silos that normalize violent discourse. Across networks of dispersed Malians, digital connectivity provides forums where polarization is fomented and that can enable access to weapons. And digital communication has been co-opted by the warring sides, who leverage internet shutdowns and digital propaganda for advantages. While discursive warfare clearly reinforces conflict dynamics and deepens social divisions, establishing a direct causal link to physical violence remains a complex and ongoing challenge that will require further investigation.

08

Private Tech Companies, the State, and the New Character of War

Emily Bienvenue, Maryanne Kelton, Zac Rogers,
Michael Sullivan, Matthew Ford

The war in Ukraine affords a window into how private tech companies are reshaping states' sovereign control over military power. State-centric models of war, where sovereign states control the battlefield and determine the technologies deployed within it, are being redefined by militaries' growing reliance in the battlespace on commercial datafication software and hardware. The war in Ukraine signals a shift in the character of armed conflict. Militaries are simultaneously decentralizing distributed decisionmaking closer to the warfighter and centralizing command and control through dependence on private tech companies that produce essential tools, including cloud computing; intelligence, surveillance, and reconnaissance (ISR) analytics; and scalable machine learning platforms for AI.[173]

The war in Ukraine is forcing conflict analysts and others to reimagine traditional state-centric models of war, as it demonstrates that militaries are no longer primarily responsible for defining the challenges of the modern battlespace and then producing tenders for technological fixes. Instead, private tech companies increasingly explain the ideal battlespace to militaries, offering software and hardware products needed to establish real-time information edges. In the Russia-Ukraine war, private companies have sought to shape Ukrainian intelligence requirements. At the beginning of Russia's invasion in February 2022, Ukraine's armed forces could not manage essential intelligence tasks. Ukraine's military lacked its own software and hardware for real-time information dominance and instead accepted support from private tech companies. These companies provide AI and big data tools that fuse intelligence and surveillance data to enhance the military's situational awareness. As the war has progressed, however, the Ukrainians have sought to develop their own government situational awareness and battle management platform called Delta.

The platform was developed as a bottom-up solution, "initially focused on a single, highly effective application: a digital map for situational awareness."[174] Over time, it expanded into a robust software ecosystem used by most of Ukraine's military, from frontline soldiers to top commanders. This in part reflects Ukraine's desire to retain direct sovereign control over what the U.S. military refers to as Combined Joint All-Domain Command and Control infrastructure (CJADC2), which manages networked sensors, data, platforms, and operations to deliver information advantages across all military services and with allies.[175]

the widespread availability of the smartphone means civilians carry around advanced sensors that can broadcast data more quickly than the armed forces themselves.

These developments are rooted in the evolution of the Internet of Things and the way that societies have embraced digital connectivity. Mass surveillance and social media now generate huge amounts of data during war. At the same time, the widespread availability of the smartphone means civilians carry around advanced sensors that can broadcast data more quickly than the armed forces themselves.[176] This enables civilians to provide intelligence to the armed forces in ways that were not previously possible.[177] Matthew Ford and Andrew Hoskins label this a "new war ecology" that is "weaponizing our attention and making everyone a participant in wars without end . . . [by] collapsing the distinctions between audience and actor, soldier and civilian, media and weapon."[178] In this ecology, warfare is participatory. Social media platforms such as TikTok, X (formerly Twitter), and Telegram are no longer merely tools for consuming war reportage; militaries accessing and processing open-source data from these platforms shapes the battlespace in real time by contributing to wider situational awareness.[179]

In this "new war ecology," Palantir Technologies is an often controversial symbol of how private tech companies and the military work together to tackle battlefield challenges.[180] Since it was founded in 2003, the company has grown quickly by providing big data software solutions. Its platforms are designed to handle complex and difficult data challenges, including those experienced by Western militaries. Importantly, Palantir's software platforms were not developed and commercialized to fulfill a military tender. They are rooted in business models prioritizing speed, flexibility, and investor return, rather than the state's national security imperatives.

As a result of their work in Ukraine, a slew of companies like Palantir have drawn media attention.[181] While commercial interests have rarely aligned neatly with geopolitics, circumstances are changing; private technology firms increasingly occupy, manage, and in some cases dominate the digital infrastructure upon which militaries now rely. States themselves have fostered this shift through selective deregulation and outsourcing of technology development. These dynamics are visible in the war in Ukraine and in the wider geopolitical contest over the global digital stack. As we argued in "Virtual Sovereignty," a paper we published in *International Affairs,* this influence has major geopolitical consequences for how states use power.[182]

Private Vendors, Public Wars

Ukraine's "new war ecology" has attracted considerable attention. In *Lessons Learned from Ukraine,* for example, military scholars John Nagle and Katie Crombe argue that private and publicly listed commercial actors have been "operationally significant" in the conduct of the war,[183] as has open-source intelligence (OSINT) for live, enhanced situational awareness and battlespace transparency.[184] Similarly, Gabriella Boyes et al. have characterized commercial vendors supplying OSINT and digitalized big data analytics as an important feature of the war, along with military reliance on private hyperlinked communication networks.[185] These authors also describe how big tech firms and ISR analytics companies stepped in soon after Russia invaded Ukraine in February 2022, providing tools and services that the Ukrainian government was either too slow or unable to deliver at scale.[186] At the beginning of Russia's invasion, this meant commercial vendors were vital to Ukraine's war effort.

By February 2024, at least eighteen U.S. private tech companies were directly supporting Ukraine's civilian and humanitarian needs or its war efforts. SpaceX, via its Starlink satellite constellation, has facilitated secure civilian and military communications after Ukraine's hardware and software infrastructures were disabled.[187] U.S. companies such as Maxar Technologies, Planet Labs, and BlackSky Technology supply ISR services, while PrimerAI and Recorded Future use AI-enabled software to provide intelligence analytics, with Recorded Future using data drawn from open web, dark web, and tech sources to provide threat insights.[188]

General Jim Hockenhull, commander of UK Strategic Command, has noted that Ukraine's insights into Russian deployments come from its capacity to integrate commercial imagery, public data, and social media analysis with the help of commercial technology.[189] Publicly available data, digitalized and processed by commercial firms, has been fed into Ukraine's war effort at scale. Even civilians participate, with Ukraine's Ministry of Digital Transformation launching the eVorog chatbot on Telegram to collect crowd-sourced intelligence from citizens.[190] TikTok and other platforms have become sites of narrative warfare, where visual and textual accounts of the war shape global perceptions and operational decisions alike. Such narrative warfare sites have created crucial data for exploitation by Palantir's software products and data fusion tools.

Ukraine's defense relies increasingly on huge volumes of civilian data stored on cloud platforms.[191] An adversary's military may supply their targeting algorithm with an individual's location, health, and online behavior. Military actors regularly mine, analyze, and repurpose social media posts.

It is not clear, however, that the deep learning systems integral to some of these new weapons can overcome the fog of war. These systems treat all data as objective representations of reality, when in fact information drawn from social media platforms is shaped by users' emotional and cognitive experiences in ways that can skew its utility for wartime intelligence.[192] The "learned knowledge" generated by analytic systems is probabilistic, not

causal—leading to the risk that algorithms are "enforc[ing] their version of 'reality' from patterns and probabilities derived from data."[193] AI trained on data taken from the internet or social media forces serious questions about the reliability and knowledge base of those models.[194] Deep learning systems can produce only a synthetic representation of reality. In this respect, "technology designed to reduce the fog of war might only make it grow denser."[195]

The problem is made worse by doubts about whether militaries like Ukraine's have the technical skills and understanding they need to properly operate these systems. Can military officers effectively evaluate the utility of heavily marketed technologies? And are they able to properly operate commercial systems already being used in the battlefield?[196] Datafication is marketed as enhancing operational effectiveness through information advantage, but its strategic value for Ukraine in the war is difficult to determine.

Geopolitical Implications of Platform Dependencies

The interdependence of state and commercial power in contemporary warfare has significant geopolitical consequences. Militaries now rely heavily on private digital infrastructures, cloud services, data analytics, AI platforms, and communications networks, to shape command, control, and perception of the battlespace. This reliance limits the decisionmaking autonomy of the state and raises new questions about sovereignty, accountability, and trust.

Global digital platforms such as TikTok and Telegram illustrate the wider environment in which these dependencies are forming. Though neither company develops military technologies, both shape the information environment surrounding war. TikTok's recommendation algorithm influences how audiences perceive the conflict in Ukraine, shaping global narratives and public opinion. Yet its complex ownership structure, rooted in Chinese parent company ByteDance and entangled with global venture capital, has sparked geopolitical concern.[197] Since 2024, U.S. policymakers have debated TikTok's national security risks, viewing its Chinese ties as potential vectors for surveillance and influence operations.[198] These concerns highlight how platforms created for civilian use can also become entangled in the political and informational dimensions of war.

However, the national security implications of global tech ownership extend far beyond TikTok. The overlapping interests of finance capital and private technology corporations transcend national borders, creating forms of influence that do not fit neatly into binary friend-or-enemy distinctions. ByteDance's global investment network, spanning Chinese state-linked entities, American private equity funds, and international investors, illustrates this transnational ownership model. It complicates national regulatory and security responses, as policymakers must ask not merely who owns a given platform, but who controls the data, infrastructure, and decisionmaking power that states increasingly depend on.[199]

Militaries face significant challenges in directing and managing the commercial actors whose global operations underpin the digital stack on which both military and civilian life depend.[200] These operational dependencies, rather than ownership structures alone, now shape the geopolitics of warfare. Microsoft's large-scale research operations in China,[201] Meta's partnership with China Mobile to build the 2Africa undersea cable,[202] Nvidia's 2025 plan for an AI research center in Shanghai,[203] and Apple's reported AI collaboration with Alibaba have all raised alarms in Washington.[204] These examples reveal how globalized research, supply chains, and infrastructure interdependence blur the boundaries between commercial innovation and national security.

The war in Ukraine exposes how the state's reliance on global commercial technologies both in defense and in information has created new vulnerabilities and blurred the boundaries of sovereignty.

Of more direct relevance to Ukraine is Telegram, a civilian encrypted messaging platform that has become central to the war's information ecosystem.[205] First associated with the 2019 Hong Kong democracy movement,[206] Telegram has been heavily relied upon by both sides in the Russia-Ukraine war for information-sharing, propaganda, and coordination, often outside official military channels.[207] Ukraine banned its official use in September 2024 because of Russia's ability to intercept or exploit data from the platform.[208] Russian authorities have likewise imposed restrictions on Telegram's functioning.[209] Telegram thus represents not a traditional defense contractor, but a global communications platform repurposed by wartime actors, highlighting how commercial technologies can be drawn into the conduct and perception of war despite their ostensibly civilian purposes.

Historically, commercial and government interests have not always aligned neatly. Yet the interdependence of state and commercial power in contemporary warfare has significant geopolitical consequences. States have encouraged this through decades of deregulation and outsourcing, but the scale, immediacy, and global reach of digital dependencies in the current era are unprecedented. The war in Ukraine exposes how the state's reliance on global commercial technologies both in defense and in information has created new vulnerabilities and blurred the boundaries of sovereignty. In response, Ukraine has sought and achieved retention of some sovereign control by utilizing its locally developed situational awareness and battle management platform, Delta, which has evolved in direct response to battlespace requirements.[210] The coming years will reveal how other armed forces adapt to the processes unleashed by the datafication of the battlefield.

Opportunism and the Imperatives of Venture Capital

Commercial actors directly embedded in Ukraine's war economy, such as Palantir, are neither neutral suppliers nor patriotic agents of state policy. Their primary motivations are commercial, shaped by venture capital imperatives, shareholder expectations, and market valuations. Analysts such as Clay Huffman and Margarita Konaev have expressed concern that firms providing essential digital capabilities for warfare may shift political or strategic allegiances if future commercial gains lie elsewhere.[211] Understanding these dynamics requires tracing the interlocking networks of global finance, political patronage, and tech entrepreneurship, linkages between U.S. tech billionaires, Silicon Valley venture capital, and political figures such as President Donald Trump, that shape how technology and national security now intersect.[212]

The growth of private capital in defense technology is striking. Bain & Company reports that between 2014 and 2023, the value of venture capital deals in the defense sector grew eighteenfold, outpacing other industries.[213] The Sagamore Institute notes that American venture capital and private equity firms have invested nearly $130 billion into defense tech since 2021—a 145 percent increase over 2017–2020 levels.[214] Much of this investment involves companies like Palantir and SpaceX, which supply operational software and infrastructure directly used in warfighting, rather than traditional Big Tech firms such as Microsoft or Amazon that provide general-purpose technologies.

These venture-backed firms view contemporary conflicts as live testing grounds. Ukraine offers both a proving space and a marketing opportunity: a site to demonstrate products under combat conditions and advertise them as "battle-tested." For instance, Palantir has claimed that its software drives most targeting in Ukraine (though independent verification remains limited).[215] It promotes its Gotham platform as capable of "harness[ing] billions of data points" to create an "AI-powered kill chain," derived from experience in the global War on Terror and Afghanistan.[216]

This illustrates a deeper shift in the relationship between the market and the military. The problem is not that defense firms are publicly traded—Lockheed Martin and General Dynamics have been for decades—but that contemporary defense-tech companies retain proprietary control over data-driven systems central to military operations. Their technologies are not merely delivered to the state; the companies are embedded in the decisionmaking architecture of warfare. When a firm's market value depends on its perceived wartime success, its incentives may diverge from those of the state it ostensibly serves. This intertwining of commercial strategy, military dependency, and investor confidence represents a new kind of vulnerability for states.

Scholars such as Elke Schwarz and Mark Howard argue that such firms are driven more by growth metrics than by public accountability or ethical restraint.[217] Even "precision targeting," marketed as reducing collateral damage, has not prevented devastating civilian casualties in Ukraine.[218] Decisions about civilian deaths remain political, but are increasingly

mediated by opaque corporate algorithms and data systems beyond direct state oversight. In this sense, the private sector's integration into the machinery of war represents not merely outsourcing but a redistribution of sovereign authority, away from the state and toward corporate actors governed by transnational capital.

Conclusion: Sovereignty in the Shadow of Silicon Valley

In 2025, well over three years into the war, Ukraine continues to face an existential struggle. Despite advances in ISR, datafication, AI, and predictive analytics, warfare remains kinetic, chaotic, and destructive. Technology has shaped decisions but not eliminated the fog or friction of war.

What is at stake, beyond the conflict itself, is the nature of state sovereignty. The ability of states to govern, defend, and act independently is increasingly mediated by private technology firms and global finance. This is not entirely new. States have long relied on private contractors, but the kind of dependency has changed. Unlike traditional arms manufacturers, today's defense-tech firms control the digital platforms, data flows, and algorithmic systems that underpin military decisionmaking. At the same time, civilian platforms like Telegram and TikTok shape the informational terrain of conflict, influencing how wars are perceived and fought.

In these circumstances, national security is no longer manufactured solely by the state. It is co-produced with private firms whose commercial interests are transnational. The challenge for states is no longer simply to confront adversaries, but to navigate their growing reliance on powerful, globally networked technology companies that underpin military and informational infrastructures alike.[219] To build the digital foundations of future warfare, militaries must understand these dependencies, and their implications for governance, accountability, and sovereignty itself.

Acknowledgments

The research documented here by academics at Flinders University has been funded by the Australian Defence Science and Technology Group since 2018 under the Strategic Research Investment-Modelling Complex Warfighting grant DST-RA-8381 and Agile Command and Control STaR Shot Theatre-level Enhanced Strategic Awareness grant DSP-RA-11320. The views expressed here are the authors' own and in the case of Emily Bienvenue do not represent the official view of the Australian Defence Department. With thanks to Steve Feldstein; Matthew Ford; participants at the Connectivity, Innovation and the Conduct of War Workshop, CEIP, Washington, DC, January 16–18, 2024; and Victor Zagorodnyuk, Flinders-DSTG research team.

About the Authors

Nate Allen is an associate professor at the Africa Center for Strategic Studies, part of the National Defense University. He's also a research fellow at the Security Institute for Governance and Leadership in Africa with Stellenbosh University. The views expressed in this paper qare those of the author and not the institutions he represents.

Rupert Barrett-Taylor has over twenty years' experience working in defense and security issues. His experience includes operational deployment as a civilian analyst and liaison officer for the UK in Afghanistan and work as an open-source analyst within the private sector. He joined the Alan Turing Institute from his second stint in the UK's Civil Service where his last role was as head of the team supporting the cross-government Integrated Security Fund with data and analytical expertise in the Foreign, Commonwealth, and Development Office.

Emily Bienvenue is a strategic advisor and research analyst with over a decade of experience supporting defense and national security decisionmaking through advanced socio-technical and strategic AI/ML risk-management frameworks. She specializes in helping organizations harness emerging technologies responsibly—balancing innovation, governance, and trust to deliver measurable capability outcomes across complex, high-stakes environments.

Mirjam de Bruijn is a professor at Leiden University in the Netherlands.

Steve Feldstein is a senior fellow at the Carnegie Endowment for International Peace in the Democracy, Conflict, and Governance Program. His research focuses on technology, national security, the global context for democracy, and U.S. foreign policy.

Matthew Ford s an associate professor in war studies at the Swedish Defence University in Stockholm. Matthew's latest book, *War in the Smartphone Age: conflict, connectivity and the crises at our fingertips*, came out with Oxford University Press in September 2025.

Maryanne Kelton is a senior lecturer in international relations at Flinders University. Since 2016, she has worked together with Australia's Department of Defence in analyzing strategic and situational awareness in the digital terrain.

Kristin Ljungkvist is an associate professor and a senior lecturer of war studies at the Swedish Defence University. Her research is broadly situated in the fields of critical security, war studies, international relations, and urban sociology. Her current research covers issues of total defence as strategy, as well as urban security and urban warfare.

Jack McDonald is a senior lecturer in war studies at the Department of War Studies, King's College London, where he is also the director of the Centre for Science and Security Studies. His current research examines the regulation of warfare and the ethical questions generated by technological change.

Jethro Norman is a senior researcher at the Danish Institute for International Studies. Primarily an ethnographer, he is concerned with bringing anthropological insights to bear on questions of international relations and political science. Broadly, he researches conflict, security, and development in conflict and post-conflict zones, and has done fieldwork in Somalia, Somaliland, Kenya, Tanzania, South Sudan and Ukraine.

Zac Rogers is a senior researcher based at Flinders University in Adelaide, Australia, currently working on a defense-funded research project examining the use of advanced data-driven decisionmaking tools by the military.

Michael Sullivan is an adjunct lecturer in international relations at the College of Business, Government and Law, Flinders University.

Gavin Wilde is a nonresident fellow in the Technology and International Affairs Program at the Carnegie Endowment for International Peace. He applies his expertise on Russia and information warfare to examine the strategic challenges posed by cyber and information operations, propaganda, and emerging technologies.

Notes

1 Matthew Ford sets this in context in his latest book, *War in the Smartphone Age: Conflict, Connectivity and the Crises at our Fingertips* (Oxford University Press, 2025).

2 Hannah Beech and Paul Mozur, "Drones Changed This Civil War, and Linked Rebels to the World," *New York Times*, May 4, 2024, https://www.nytimes.com/2024/05/04/world/asia/myanmar-war-drones.html.

3 Rebecca Tan, Caleb Quinley, and Yan Naing, "Myanmar Military Unleashes Drones to Counter Rebel Advances," *Washington Post*, October 12, 2024, https://www.washingtonpost.com/world/2024/10/12/myanmar-civil-war-drones.

4 Su Mon, "The War From the Sky: How Drone Warfare Is Shaping the Conflict in Myanmar," ACLED, July 1, 2025, https://acleddata.com/report/war-sky-how-drone-warfare-shaping-conflict-myanmar.

5 Rupert Barrett-Taylor and Gavin Wilde, "A Digitized, Efficient Model of War," Carnegie Endowment for International Peace, June 3, 2025, https://carnegieendowment.org/research/2025/06/a-digitized-efficient-model-of-war?lang=en.

6 Nate Allen, "Digital Technology, Strategic Adaptation, and the Outcomes of Twenty-First Century Armed Conflict," Carnegie Endowment for International Peace, June 17, 2025, https://carnegieendowment.org/research/2025/06/digital-technology-strategic-adaptation-and-the-outcomes-of-twenty-first-century-armed-conflict?lang=en.

7 Aurel Sari, "War and Law in a Digital World," Carnegie Endowment for International Peace, June 26, 2025, https://carnegieendowment.org/research/2025/06/war-and-law-in-a-digital-world?lang=en.

8 Jethro Norman, "Foreign Fighters 2.0: The Interplay of Technology and Lived Experience in the Russia-Ukraine War," Carnegie Endowment for International Peace, July 8, 2025, https://carnegieendowment.org/research/2025/07/foreign-fighters-russia-ukraine-technology?lang=en.

9 Jack McDonald, "Digital Connectivity and Digital Informants in War," Carnegie Endowment for International Peace, July 31, 2025, https://carnegieendowment.org/research/2025/07/digital-connectivity-and-digital-informants-in-war?lang=en.

10 Kristin Ljungkvist, "Participatory War and Its Challenges for Total Defense," Carnegie Endowment for International Peace, August 13, 2025, https://carnegieendowment.org/research/2025/08/participatory-war-and-its-challenges-for-total-defense?lang=en.

11 Mirjam de Bruijn, "Digital Communication as a Weapon: The Case of Mali," Carnegie Endowment for International Peace, October 14, 2025, https://carnegieendowment.org/research/2025/10/digital-communication-as-a-weapon-mali?lang=en.

12 Emily Bienvenue, et al., "Private Tech Companies, the State, and the New Character of War," Carnegie Endowment for International Peace, December 1, 2025, https://carnegieendowment.org/research/2025/12/ukraine-war-tech-companies?lang=en.

13 Jason Blakely, *We Built Reality: How Social Science Infiltrated Culture, Politics, and Power* (Oxford University Press, 2020), 128.

14 Martin Van Creveld, *Technology and War: From 2000 B.C. to the Present* (Touchstone, 2010), 246; Jill Lepore, *If, Then: How the Simulmatics Corporation Invented the Future* (Liverlight, 2020), 3-4.

15 Geoffrey A. Fowler, "I Let ChatGPT›s New ‹Agent› Manage My Life. It Spent $31 on a Dozen Eggs," *Washington Post*, February 7 2025, https://www.washingtonpost.com/technology/2025/02/07/openai-operator-ai-agent-chatgpt; Ian Sherr, "Glue in Pizza? Eat Rocks? Google's AI Search Is Mocked for Bizarre Answers," *CNET*, May 24 2024. https://www.cnet.com/tech/services-and-software/glue-in-pizza-eat-rocks-googles-ai-search-is-mocked-for-bizarre-answers/#ftag=MSF491fea7.

16 Euan McKirdy, "Lion Air Crash: Pilots Fought Automatic Safety System Before Plane Plunged," *CNN,* November 28, 2018, https://www.cnn.com/2018/11/28/asia/lion-air-preliminary-report-intl/index.html.

17 Stephanie Carvin, "How Not to War," *International Affairs,* September 2022, https://academic.oup.com/ia/article/98/5/1695/6686651.

18 James C. Scott, *Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed* (Yale University Press, 2020), 311, 327.

19 David Omand, Jamie Bartlett, & Carl Miller, "Introducing Social Media Intelligence (SOCMINT)," *Intelligence and National Security* 27, no. 6 (2012): 801–823. https://doi.org/10.1080/02684527.2012.716965.

20 Elting Morison, *Men, Machines, and Modern Times* (MIT Press, 1966), 211.

21 James Cody, "AWPD-42 to Instant Thunder: Consistent, Evolutionary Thought or Revolutionary Change?," Maxwell Air Force Base School of Advanced Airpower Studies, May 1, 1996, https://apps.dtic.mil/sti/tr/pdf/ADA424862.pdf.

22 John Correll, "Igloo White," *Air Force Magazine,* November 2004, https://www.airandspaceforces.com/PDF/MagazineArchive/Documents/2004/November%202004/1104igloo.pdf.

23 United States Department of the Army, "U.S. Army Operational Concept: The Airland Battle and Corps 86," no. 525 5 *TRADOC Pam,* 1981, https://cgsc.contentdm.oclc.org/digital/collection/p4013coll9/id/656.

24 See John Arquilla and David Ronfeldt, "Cyberwar is Coming!," RAND Corporation, 1993, https://www.rand.org/pubs/reprints/RP223.html.

25 Amos C. Fox, "Precision Paradox and Myths of Precision Strike in Modern Armed Conflict." *The RUSI Journal* 169, nos. 1–2 (2024): 62–74. https://doi.org/10.1080/03071847.2024.2343717.

26 *Ibid.*

27 Stanley McCrystal, "It Takes a Network," *Foreign Policy, February 21, 2011,* https://foreignpolicy.com/2011/02/21/it-takes-a-network.

28 Harry Davies, Bethan McKernan and Dan Sabbagh, "'The Gospel': How Israel Uses AI to Select Bombing Targets in Gaza," *The Guardian,* December 1, 2023, https://www.theguardian.com/world/2023/dec/01/the-gospel-how-israel-uses-ai-to-select-bombing-targets; Hanna Duggal, Mohammed Hussein and Shakeeb Asrar, "Israel's Attacks on Gaza: The Weapons and Scale of Destruction," *Al Jazeera,* November 9, 2023, https://www.aljazeera.com/news/longform/2023/11/9/israel-attacks-on-gaza-weapons-and-scale-of-destruction.

29 Anthony Cordesman, "The Real Revolution in Military Affairs," August 5, 2014, Center for Strategic and International Studies, https://www.csis.org/analysis/real-revolution-military-affairs.

30 Gavin Wilde, "Technology Alone Won't Break the Stalemate in Ukraine," *Foreign Policy,* March 19, 2024, https://foreignpolicy.com/2024/03/19/technology-ai-drones-stalemate-ukraine-russia-manpower.

31 Simon Winchester, *The Perfectionists: How Precision Engineers Created the Modern World*, (HarperCollins, 2018), 16.

32 Richard Nelson, "Physics Envy: Get Over It," *Issues in Science and Technology,* Spring 2015, https://issues.org/physics-envy-get-over-it.

33 N. Katherine Hayles, *How We Became Post-Human: Virtual Bodies in Cybernetics, Literature, and Informatics* (University of Chicago Press, 1999), 231-232.

34 David Beer, *The Data Gaze: Capitalism, Power and Perception* (SAGE Publications Ltd, 2019), 25.

35 Scott refers to this as "*metis.*" See James Plunkett, "Metis Matters," Medium, August 7, 2024, https://medium.com/@jamestplunkett/metis-matters-6a48270c2731.

36 Scott, *Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed,* 309.

37 See Christopher Sims, "The Human Terrain System: Operationally Relevant Social Science Research in Iraq and Afghanistan," U.S. Army War College Press, December 1, 2015, https://press.armywarcollege.edu/monographs/6/.

38 Frederick W. Taylor, *The Principles of Scientific Management* (Harper, 1911).

39 Martin Heidegger, *The Question Concerning Technology and Other Essays,* ed. W. Lovitt (Harper & Row), 36f.

40 Nolen Gertz, *Nihilism and Technology* (Rowman & Littlefield, 2018), 106.

41 Hubert Dreyfus, "Heidegger and Foucault on the Subject, Agency and Practices," University of California, 2002, http://socrates.berkeley.edu/~hdreyfus/html/paper_heidandfoucault.html.

42 Van Creveld, *Technology and War: From 2000 B.C. to the Present,* 319.

43 *Ibid.,* 242-243.

44 See Richard Danzig, "Machines, Bureaucracies, and Markets as Artificial Intelligences," Center for Security and Emerging Technology, January 2022, https://cset.georgetown.edu/publication/machines-bureaucracies-and-markets-as-artificial-intelligences and Michael Mazarr, "Abstract Systems, Social Trust, and Institutional Legitimacy," *American Affairs Journal,* Spring 2022, https://americanaffairsjournal.org/2022/02/abstract-systems-social-trust-and-institutional-legitimacy.

45 Gertz, *Nihilism and Technology,* 106.

46 Amanda Mull, "Self-Checkout Is a Failed Experiment," *The Atlantic,* October 18, 2023, https://www.theatlantic.com/technology/archive/2023/10/self-checkout-kiosks-grocery-retail-stores/675676/

47 Dan Davies, *The Unaccountability Machine* (Profile Books, 2024).

48 Gavin Wilde, "The Path to War is Paved by Obscure Intentions: Signaling and Perception in the Era of AI," *Just Security,* October 20, 2023, https://www.justsecurity.org/89641/the-path-to-war-is-paved-with-obscure-intentions-signaling-and-perception-in-the-era-of-ai.

49 Astrid H.M. Nordin and Dan Oberg, "Targeting the Ontology of War: From Clausewitz to Baudrillard," *Millennium-Journal of International Studies 43,* no. 2 (2015): 392–410. https://doi.org/10.1177/0305829814552435.

50 Morison, *Men, Machines, and Modern Times,* 211.

51 Stephen Biddle, "Back in the Trenches: Why New Technology Hasn't Revolutionized Warfare in Ukraine," *Foreign Affairs* 102 (September/October 2023): https://www.foreignaffairs.com/ukraine/back-trenches-technology-warfare.

52 Michael C. Horowitz, "Artificial Intelligence, International Competition, and the Balance of Power," *Texas National Security Review* 1, no. 3 (2018): 36–57, https://tnsr.org/2018/05/artificial-intelligence-international-competition-and-the-balance-of-power.

53 Audrey K. Cronin, "Technology and Strategic Surprise: Adapting to an Era of Open Innovation," *Parameters* 50, no. 3 (2020): https://press.armywarcollege.edu/parameters/vol50/iss3/8.

54 Matt Burgess, "A Mysterious Satellite Hack Has Victims Far Beyond Ukraine," *Wired,* March 23, 2022, https://www.wired.com/story/viasat-internet-hack-ukraine-russia.

55 "Elon Musk's Starlink Arrives in Ukraine but What Next?," BBC News, March 1, 2022, https://www.bbc.com/news/technology-60561162.

56 "How Elon Musk's Satellites Have Saved Ukraine and Changed Warfare," *Economist*, January 5, 2023, https://www.economist.com/briefing/2023/01/05/how-elon-musks-satellites-have-saved-ukraine-and-changed-warfare.

57 "The Degrading Treatment of Ukraine's Internet," *Economist*, March 26, 2022, https://www.economist.com/science-and-technology/2022/03/26/the-degrading-treatment-of-ukraines-internet.

58 "The Degrading Treatment of Ukraine's Internet," *Economist*.

59 Jonathan Beale, "Ukraine War: How Old Tech Is Helping Ukraine Avoid Detection," BBC News, May 3, 2023, https://www.bbc.com/news/world-europe-65458263.

60 Alan Yuhas, Thomas Gibbons-Neff, and Yousur Al-Hlou, "For Russian Troops, Cellphone Use Is a Persistent, Lethal Danger," *New York Times,* January 3, 2023, https://www.nytimes.com/2023/01/04/world/europe/ukraine-russia-cellphones.html.

61 Kevin Freese, "Smart Phones Playing Prominent Role in Russia-Ukraine War," United States Army Training and Doctrine Command, August 10, 2023, https://oe.tradoc.army.mil/2023/08/10/smart-phones-playing-prominent-role-in-russia-ukraine-war.

62 "Telegram Has Become a Key Tool for the Russian Military. Why Does Moscow Continue to Rely on a Dubai-based Civilian Messaging App?," Meduza, August 28, 2024, https://meduza.io/en/feature/2024/08/28/telegram-has-become-a-key-tool-for-the-russian-military-why-does-moscow-continue-to-rely-on-a-dubai-based-civilian-messaging-app.

63 "Telegram Has Become a Key Tool for the Russian Military," Meduza.

64 Adam Satariano and Paul Mozer, "Russia, in New Push, Increasingly Disrupts Ukraine's Starlink Service," *New York Times*, March 25, 2024, https://www.nytimes.com/2024/05/24/technology/ukraine-russia-starlink.html.

65 "Nigeria: Mobile-Cellular Subscriptions per 100 People," International Telecommunications Union, 2024, https://datahub.itu.int/data/?i=178&e=NGA&v=chart&u=per+100+people.

66 Aliyu Odamah Musa, "Socio-Economic Incentives, New Media and the Boko Haram Campaign of Violence in Northern Nigeria*," Journal of African Media Studies* 4, no. 1 (2012): https://doi.org/10.1386/jams.4.1.111_1, 121.

67 Jacob Udo-Udo Jacob and Idorenyin Akpan, "Silencing Boko Haram: Mobile Phone Blackout and Counterinsurgency in Nigeria's Northeast Region," *Stability: International Journal of Security and Development* 4, no. 1 (2015): https://stabilityjournal.org/articles/10.5334/sta.ey, 4–5.

68 Jacob and Akpan, "Silencing Boko Haram," 8.

69 IRIN News, "Military's Shutdown of NE Nigeria Telecoms Disrupts Trade," New Humanitarian, June 11, 2013, https://www.thenewhumanitarian.org/news/2013/06/11/military-s-shutdown-ne-nigeria-telecoms-disrupts-trade.

70 Jacob and Akpan, "Silencing Boko Haram," 11.

71 Freedom Onuoha, "Understanding Boko Haram's Attacks on Telecommunication Infrastructure," in Ioannis Mantzikos, ed., *Boko Haram: The Anatomy of a Crisis,* E-International Relations (2013): https://www.e-ir.info/publication/boko-haram-anatomy-of-a-crisis, 16–26.

72 Njadvara Musa and Ann Godwin, "Telecoms Firms Fume as Boko Haram Destroys Masts in Yobe," *Guardian*, February 18, 2020, https://guardian.ng/news/telecoms-firms-fume-as-boko-haram-destroys-masts-in-yobe.

73 Jacob and Akpan, "Silencing Boko Haram," 14.

74 Simon Kemp, "Digital Somalia: 2024," February 23, 2024, https://datareportal.com/reports/digital-2024-somalia.

75 Christopher Anzalone, "Continuity and Change: The Evolution and Resilience of Al-Shabaab's Media Insurgency, 2006–2016," Hate Speech International (2016): 30.

76 Reserve Officers Association, "Keynote Address by Terrence Ford," Foreign Policy Research Institute, September 27, 2010, https://www.youtube.com/watch?v=CTNvXZl0bjw.

77 Ken Menkhaus, "Al-Shabaab and Social Media: A Double-Edged Sword," *Brown Journal of World Affairs* 20 (2013): 309–330, https://bjwa.brown.edu/20-2/al-shabaab-and-social-media-a-double-edged-sword; and Anzalone, "Continuity and Change."

78 Shira Frenkel and Ben Hubbard, "After Social Media Bans, Militant Groups Found Ways to Remain," *New York Times*, April 19, 2018, https://www.nytimes.com/2019/04/19/technology/terrorist-groups-social-media.html.

79 Dan Joseph and Harun Maruf, *Inside Al-Shabaab: The Secret History of Al-Qaeda's Most Powerful Ally* (Bloomington: Indiana University Press, 2018): 234–35.

80 Menkhaus, "Al-Shabaab and Social Media," 323.

81 "Letter Dated 7 November 2018 from the Chair of the Security Council Committee Pursuant to Resolutions 751 (1992) and 1907 (2009) Concerning Somalia and Eritrea Addressed to the President of the Security Council," United Nations, S/2018/100, https://digitallibrary.un.org/record/1652108, 156.

82 "Al-Shabaab's Digital Expansion: A New Era of Terror Propaganda," Tactics Institute for Security and Counter Terrorism, August 6, 2024, https://tacticsinstitute.com/analysis/al-shabaabs-digital-expansion-a-new-era-of-terror-propaganda.

83 Moustafa Ayad, Anisa Harrasy, and Mohammed Abdullah, "Under-Moderated,Unhinged and Ubiquitous: Al-Shabaab and the Islamic State Networks on Facebook," Institute of Strategic Dialogue, 2022, https://www.isdglobal.org/isd-publications/under-moderated-unhinged-and-ubiquitous-al-shabaab-and-the-islamic-state-networks-on-facebook, 7.

84 See David Patrikarakos, *War in 140 Characters: How Social Media is Reshaping Conflict in the Twenty-First Century* (Basic Books, 2017); and P. W. Singer and Emerson T. Brooking, *Likewar: The Weaponization of Social Media* (Houghton Mifflin Harcourt, 2018).

85 Matthew Ford and Andrew Hoskins, *Radical War: Data, Attention and Control in the 21st Century* (Hurst, 2022).

86 *Legality of the Threat or Use of Nuclear Weapons* (Advisory Opinion) (1996) International Court of Justice Rep. 226, para. 78 (describing distinction as a "cardinal" principle of the law of armed conflict).

87 Carl von Clausewitz, *On War* (Princeton University Press, 1976), 87.

88 Clausewitz, *On War*, 604.

89 Diplomatic Conference on the Reaffirmation and Development of International Humanitarian Law Applicable in Armed Conflicts, "Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Additional Protocol I)," June 8, 1977, Article 51(3).

90 For example, see "Ukraine War: Romania Reveals Russian Drone Parts Hit Its Territory," BBC News, September 6, 2023, https://www.bbc.co.uk/news/world-europe-66727788.

91 Elsa Court, "Military Intelligence Hacks Russian Tax Authorities," *Kyiv Independent*, December 12, 2023, https://kyivindependent.com/military-intelligence-hacks-russian-tax-authorities.

92 See also Kubo Mačák, "Nothing Is Certain but Death and Taxes (Unless You Get Hacked): An International Law Perspective on Ukraine's Cyber Attack Against Russia's Federal Tax Service," EJIL:Talk, December 14, 2023, https://www.ejiltalk.org/nothing-is-certain-but-death-and-taxes-unless-you-get-hacked-an-international-law-perspective-on-ukraines-cyber-attack-against-russias-federal-tax-service.

93 "Military Objectives," International Cyber Law Interactive Toolkit, accessed September 27, 2024, https://cyberlaw.ccdcoe.org/wiki/Military_objectives#Qualification_of_data_as_an_object_under_IHL.

94 Diplomatic Conference on the Reaffirmation and Development of International Humanitarian Law Applicable in Armed Conflicts, "Additional Protocol I," Article 49(1).

95 Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* 2nd edition (Cambridge University Press, 2017), *Cf.* Rule 92(3).

96 On the notion of legal narratives, see Aurel Sari, "Norm Contestation for Strategic Effect: Legal Narratives as Information Advantage" *Zeitschrift für ausländisches öffentliches Recht und Völkerrecht* (2023): 119–154, 125–133.

97 See Michael N. Schmitt, "Normative Architecture and Applied International Humanitarian Law," *International Review of the Red Cross* (2022): 2097–2110, 2108.

98 Gregory Asmolov, "The Transformation of Participatory Warfare: The Role of Narratives in Connective Mobilization in the Russia–Ukraine War," *Digital War* 3, no. 1 (2022): 25–37, https://doi.org/10.1057/S42984-022-00054-5; and Olga Boichak and Andrew Hoskins, "My War: Participation in Warfare," *Digital War* 3, no. 1 (2022): 1–8, https://doi.org/10.1057/s42984-022-00057-2.

99 Matthew Ford and Andrew Hoskins, *Radical War: Data, Attention and Control in the Twenty-First Century* (Oxford University Press, 2022).

100 Asmolov, "The Transformation of Participatory Warfare"; and Boichak and Hoskins, "My War."

101 Tetyana Lokot, "Public Networked Discourses in the Ukraine-Russia Conflict: 'Patriotic Hackers' and Digital Populism," Irish Studies in International Affairs 28, no. 1 (2017): 99–116, https://doi.org/10.1353/isia.2017.0011; and Ilmari Käihkö, "Conflict Chatnography: Instant Messaging Apps, Social Media and Conflict Ethnography in Ukraine," Ethnography 21, no. 1 (2020): 71–91, https://doi.org/10.1177/1466138118781640.

102 David Malet, *Foreign Fighters: Transnational Identity in Civil Conflicts* (Oxford University Press, 2013); and Thomas Hegghammer, "The Rise of Muslim Foreign Fighters: Islam and the Globalization of Jihad," International Security 35, no. 3 (2010): 53–94, https://doi.org/10.1162/ISEC_a_00023.

103 Jethro Norman, "War Volunteers in the Digital Age: How New Technologies Transform Conflict Dynamics," Danish Institute for International Studies (Policy Brief 2024), July 2024, http://dx.doi.org/10.13140/RG.2.2.25050.56003; and Matthew Ford, "From Innovation to Participation: Connectivity and the Conduct of Contemporary Warfare," *International Affairs* 100, no. 4: 1531–1549, https://doi.org/10.1093/ia/iiae061.

104 Roman Horbyk, "'The War Phone': Mobile Communication on the Frontline in Eastern Ukraine," *Digital War 3,* no. 1 (2022): 9–24, https://doi.org/10.1057/S42984-022-00049-2.

105 Jethro Norman, Matthew Ford, and Signe Marie Cold-Ravnkilde, "Smartphones: The Crisis in the Palm of Our Hand," *International Affairs* 100, no. 4 (July 2024): 1361–1379, https://doi.org/10.1093/ia/iiae128.

106 Nicolas Niarchos, "A Russian Strike Kills Foreign Fighters in Ukraine," *The Nation,* March 15, 2022, https://www.thenation.com/article/world/lviv-foreign-fighters-ukraine/.

107 David Edgerton, *The Shock of the Old: Technology and Global History Since 1900* (Oxford University Press, 2007).

108 Arthur Snell, host, *Behind the Lines with Arthur Snell*, podcast, season 3, episode 8, "Digital War - From Ukraine, to the Sahel," Swedish National Defence University, October 21, 2023, https://research.diis.dk/en/publications/behind-the-lines-with-arthur-snell-digital-war-from-ukraine-to-th.

109 Shane Darcy, *To Serve the Enemy: Informers, Collaborators, and the Laws of Armed Conflict* (Oxford University Press, 2019).

110 Matthew Ford and Andrew Hoskins, *Radical War: Data, Attention and Control in the Twenty-First Century* (Hurst & Co., 2022).

111 Matthew Ford, "The Open Kill Chain: Military Targeting in an Era of Participative War," forthcoming, 2025.

112 Ford, "The Open Kill Chain."

113 Darcy, *To Serve the Enemy*.

114 Fikire Tinsae Birhane, "Targeting of Children in Non-International Armed Conflicts," *Journal of Conflict and Security Law* 26, no. 2 (2021): 377–400.

115 Darcy, *To Serve the Enemy*.

116 Kubo Mačák, "Will the Centre Hold? Countering the Erosion of the Principle of Distinction on the Digital Battlefield," *International Review of the Red Cross* 105 (2023): 965–91.

117 Mačák, "Will the Centre Hold?"

118 Jack McDonald, "Information, Privacy, and Just War Theory," *Ethics & International Affairs* 34, no. 3 (2020): 379–400.

119 Cécile Fabre, "Guns, Food, and Liability to Attack in War," *Ethics* 120, no. 1 (2009): 36–63.

120 NATO Cooperative Cyber Defence Centre of Excellence, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, ed. Michael N. Schmitt (Cambridge University Press, 2013).

121 International Committee of the Red Cross, "Protecting Civilians Against Digital Threats During Armed Conflict: Recommendations to States, Belligerents, Tech Companies, and Humanitarian Organizations," 2023.

122 Michael N. Schmitt and William Casey Biggerstaff, "Ukraine Symposium – Are Civilians Reporting With Cell Phones Directly Participating in Hostilities?," *Articles of War,* Lieber Institute West Point, November 2022, https://lieber.westpoint.edu/civilians-reporting-cell-phones-direct-participation-hostilities.

123 Mačák, "Will the Centre Hold?"

124 Anthony King, "Digital Targeting: Artificial Intelligence, Data, and Military Intelligence," *Journal of Global Security Studies* 9, no. 2 (June 2024): https://doi.org/10.1093/jogss/ogae009.

125 Lukasz Olejnik, "Smartphones Blur the Line Between Civilian and Combatant," *Wired*, June 2022, https://www.wired.com/story/smartphones-ukraine-civilian-combatant.

126 Stuart Gordon, "The Protection of Civilians: An Evolving Paradigm?," *Stability: International Journal of Security & Development* 2, no. 2 (2013): 1–16.

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

128 Jan Angstrom and Kristin Ljungkvist, "Unpacking the Varying Strategic Logics of Total Defence," *Journal of Strategic Studies* 47 no. 4 (2023): 498–522.

129 Matthew Ford, *War in the Smartphone Age: Conflict, Connectivity and the Crises at Our Fingertips* (Hurst & Company, 2025).

130 See, for example, Sascha-Dominik Bachmann, "Hybrid Threats, Cyber Warfare and NATO's Comprehensive Approach for Countering 21st Century Threats: Mapping the New Frontier of Global Risk and Security Management," *Amicus Curiae* 88 (2011): 24–27; Mikael Weissmann, Niklas Nilsson, and Björn Palmertz, "Moving Out of the Blizzard: Towards a Comprehensive Approach to Hybrid Threats and Hybrid Warfare," in Mikael Weissmann, Niklas Nilsson, Björn Palmertz, and Per Thunholm (eds), *Hybrid Warfare: Security and Asymmetric Conflict in International Relations* (London: I.B. Tauris, Bloomsbury Collections, 2021), 263–272; Ieva Berzina, "From 'Total' to 'Comprehensive' National Defence: The Development of the Concept in Europe," *Journal on Baltic Security* 6, no. 2 (2020): pp. 7–15; Jonny Hall and Hugh Sandeman, "NATO's Resilience: The First and Last Line of Defence," *LSE IDEAS Strategic Update*, May 9, 2022, https://lseideas.medium.com/natos-resilience-the-first-and-last-line-of-defence-89c42ac47eb0; and Center for Strategic and International Studies, "Whole of Society Resilience Lessons from Russia-Ukraine. Conflict in Focus," 2025, https://www.csis.org/analysis/whole-society-resilience-lessons-russia-ukraine-conflict-focus.

131 Axel Hagelstam, "Cooperating to Counter Hybrid Threats," *NATO Review,* November 23, 2018, https://www.nato.int/docu/review/articles/2018/11/23/cooperating-to-counter-hybrid-threats/index.html.

132 Hanna Shelest, "Defend. Resist. Repeat: Ukraine's Lessons for European Defence," European Council on Foreign Relations, November 2022, https://ecfr.eu/wp-content/uploads/2022/11/Defend.-Resist.-Repeat-Ukraines-lessons-for-European-defence.pdf.

133 Oren Liebermann, "How Ukraine Is Using Resistance Warfare Developed by the US to Fight Back Against Russia," CNN, August 27, 2022, https://edition.cnn.com/2022/08/27/politics/russia-ukraine-resistance-warfare/index.html.

134 See, for example, Ishaan Tharoor, "Ukraine's Resilience Sets a Global Standard," *Washington Post,* December 14, 2022, https://www.washingtonpost.com/world/2022/12/14/ukraine-resilience-global-standard; and Nicholas Krohley, "Ukrainian Civilians Are Pioneering the Art of Resistance," *Foreign Policy,* February 28, 2024, https://foreignpolicy.com/2024/02/28/ukrainian-civilian-resistance-movements-women-war-mavkas.

135 Matthew Ford, "From Innovation to Participation: Connectivity and the Conduct of Contemporary Warfare," *International Affairs* 100, no. 4 (July 2024): 1,531–1,549.

136 Matthew Ford, "Ukraine, Participation and the Smartphone at War," *Political Anthropological Research on International Social Sciences* 4, no. 2 (2023): 219–247; and Ford, *War in the Smartphone Age*.

137 Kristin Ljungkvist, "The Military-Strategic Rationality of Hybrid Warfare: Everyday Total Defence Under Strategic Non-peace in the Case of Sweden," *European Journal of International Security* 9, no. 4 (2024): 533–552.

138 Swedish Government, "Totalförsvaret 2021–2025. Prop. 2020/21:30," 2020, https://www.regeringen.se/rattsliga-dokument/proposition/2020/10/prop.-20202130, 137.

139 Matthew Ford and Andrew Hoskins, *Radical War. Data, Attention and Control in the 21st Century* (London: Hurst & Company, 2022).

140 See, for example, Swedish Defence Commission, "Ds 2017:66 Motståndskraft. Inriktningen av totalförsvaret och utformningen av det civila försvaret 2021–2025," 2017, https://www.regeringen.se/globalassets/regeringen/dokument/forsvarsdepartementet/forsvarsberedningen/ds-2017-66-motstandskraft-inriktningen-av-totalforsvaret-och-utformningen-av-det-civila-forsvaret-2021-20252.pdf, 67.

141 Gina Gustavsson, *Du stolta, du fria: Om svenskarna, Sverigebilden och folkhälsopatriotismen* (Stockholm: Kaunitz-Olsson, 2021); Sveriges Radio, 'Dold Facebookgrupp försöker påverka svenska intressen utomlands' (2021), https://sverigesradio.se/artikel/dold-facebookgrupp-forsoker-paverka-svenska-intressen-utomlands.

142 David Alexander, "From Civil Defence to Civil Protection – and Back Again," *Disaster Prevention and Management* 11, no. 3 (2002): 209–2013.

143 Alexander, "From Civil Defence to Civil Protection," 210.

144 Ford, "Ukraine, Participation and the Smartphone at War.".

145 Aurel Sari, "War and Law in a Digital World," *Carnegie Endowment for International Peace*, June 26, 2025, https://carnegieendowment.org/research/2025/06/war-and-law-in-a-digital-world; Jack McDonald, "Digitla Connectivity and Digital Informants in War," *Carnegie Endowment for International Peace*, July 31, 2025, https://carnegieendowment.org/research/2025/07/digital-connectivity-and-digital-informants-in-war?lang=en.

146 Ford, "Ukraine, Participation and the Smartphone at War."

147 Pontus Winther and Per-Erik Nilsson, "Smart Tactics or Risky Behaviour? The Lawfulness of Encouraging Civilians to Participate in Targeting in an Age of Digital Warfare," Hague Centre for Strategic Studies (2023): https://www.jstor.org/stable/pdf/resrep49622.pdf

148 Winther and Nilsson, "Smart Tactics or Risky Behaviour?"

149 William Merrin, *Digital War: A Critical Introduction* (Routledge Taylor & Francis Group, 2019), Chapter 10, 195–218.

150 Matthew Ford and Andrew Hoskins, *Radical War: Data, Attention and Control in the Twenty-First Century*, 1st ed. (Oxford University Press, 2022).

151 Johan Galtung, "Cultural Violence," *Journal of Peace Research* 27, no. 3 (August 1, 1990): 291–305, https://doi.org/10.1177/0022343390027003005.

152 This refers to the following research projects that I led: "Connecting in Times of Duress," 2012 to 2019, https://www.connecting-in-times-of-duress.nl/; "Decoding Digital Media in African Conflict" (DDMAC), 2021 to 2024, https://decodingdigitalmedia.org/; and "Digital Warfare in the Sahel," 2023 to 2028, https://www.universiteitleiden.nl/en/research/research-projects/humanities/digital-warfare-in-the-sahel-popular-networks-of-war-and-cultural-violence.

153 For an excellent description of the conflict in Mali and the Sahel, see Alexander Thurston, *Jihadists of North Africa and the Sahel: Local Politics and Rebel Groups*, 1st ed. (Cambridge University Press, 2020), https://doi.org/10.1017/9781108771160; and Alexander Thurston, "Conflict in the Sahel," in *African Studies*, by Alexander Thurston (Oxford University Press, 2024), https://doi.org/10.1093/obo/9780199846733-0232.

154 "Mali," International Telecommunication Union, accessed August 25, 2025, https://datahub.itu.int/data/?e=MLI&Affordability=Interconnection.

155 Simon Kemp, "Digital 2025: Mali," DataReportal, March 3, 2025, https://datareportal.com/reports/digital-2025-mali.

156 Most computational research on social media and conflict has been centered on Twitter, which previously allowed researchers to scrape and analyze platform data. However, because of recent policy changes, this access is no longer permitted. This research was part of the project DDMAC that run from 2021 to 2024.

157 Daniel Thilo Schroeder et al., "Social Media in the Global South: A Network Dataset of the Malian Twittersphere," *Journal of Data Mining & Digital Humanities* (November 3, 2023): https://doi.org/10.46298/jdmdh.11246; and Mirjam de Bruijn et al., "'Aren't We All Journalists?' Citizen Journalism, Disinformation and the Weaponization of Social Media in Conflict Torn Mali," *Journalism* 26, no. 5 (January 6, 2025): https://doi.org/10.1177/14648849241312743.

158 Mamadou Togola and Mirjam de Bruijn, "Les Réseaux Sociaux Dans La Dynamique Des Conflits Au Centre Du Mali: Un Exemple de Journalisme Citoyen à Travers La Plateforme Numérique KI," *Canadian Journal of African Studies / Revue Canadienne Des Études Africaines* 57, no. 2 (May 4, 2023): 305–325, https://doi.org/10.1080/00083968.2023.2177689.

159 Researching WhatsApp use presented several challenges, primarily because of the platform's design as a private, end-to-end encrypted messaging service. This made it impossible to scrape or access content through traditional digital methods. Instead, researchers adopted an ethnographic approach, relying on permission to join closed or private groups.

160 Modibo Cissé, "WhatsApp Platform for the People: The Conflict in Central Mali and Community Leaders Online," in *Media Forerunners, Emerging Socio-Political Youth Leadership in Times of Conflict and Digitization,* eds. Mirjam de Bruijn and Bruce Mutsvairo (Berlin: De Gruyter), forthcoming.

161 Togola and de Bruijn, "Les Réseaux Sociaux Dans La Dynamique Des Conflits Au Centre Du Mali."

162 Mirjam de Bruijn and Luca Bruls, "Social Media and Conflict in Mali," *Conflict and Society*, forthcoming 2025.

163 Luca Bruls and Aissa Dite Essi Pengoulba, "Thriving on TikTok in Mali: the Generation of Influencers," *Voice4Thought,* September 15, 2023, https://voice4thought.org/thriving-on-tiktok-in-mali-the-generation-of-influencers/.

164 Johannes Fabian, "Forgetful Remembering: A Colonial Life in the Congo," *Africa: Journal of the International African Institute* 73, no. 4 (2003).

165 Signe Marie Cold-Ravnkilde and Almamy Sylla, "The Rise of Mali's 'Videomen' as Cybercombatants in Global Crisis Ecologies," *International Affairs* 100, no. 4 (July 10, 2024): 1405–1429, https://doi.org/10.1093/ia/iiae121.

166 Matthew Ford and Gregory Asmolov, "The Open Kill Web: Military Targeting in an Era of Participative Warfare," forthcoming in 2026.

167 Matthew Ford, *War in the Smartphone Age* (London: Hurst & Co, 2025).

168 Kaatiba Macina has been seriously militarily active in central Mali since 2015. It controls a large part of northern and central rural Mali. Kaatiba Macina consists of numerous armed groups, most of which are homegrown and have a Salafi ideology. The groups are defined as terrorists by the state, as opposed to being characterized as a rural insurgency that is also a local resistance movement against the state and its historical role in the region. See Thurston *Jihadists of North Africa and the Sahel* and "Conflict in the Sahel"; and Han van Dijk and Mirjam de Bruijn, "Religious Movements in the Drylands: Ethnicity, Jihadism, and Violent Extremism," in *Drylands Facing Change* (Routledge, 2022).

169 Many cities fell into this plight, such as Farabougou, Moura, and Tombouctou.

170 See "How New Technologies Shape Conflict – the Case of Social Media" (2021) from International Crisis Group, which mentions the influence of social media in informing polarizing tendencies and confirms our own observations in Mali, https://www.crisisgroup.org/global/how-new-technologies-shape-conflict-case-social-media.

171 Luca Bruls, "Shifting Attention From Conflict to TikTok in Mali," *Media Forerunners, Emerging Socio-Political Youth Leadership in Times of Conflict and Digitization*, eds. Mirjam de Bruijn and Bruce Mutsvairo (De Gruyter, forthcoming).

172 These ethnographic observations are confirmed in reports such as Europol's 2023 review report on jihadist online propaganda. See "Online Jihadist Propaganda: 2023 in Review," Europol, 2024, https://www.europol.europa.eu/cms/sites/default/files/documents/Online_jihadist_propaganda_2023_in_review.pdf; and "Briefing: Al-Qaeda's Sahel Branch Issues Deluge of Ramadan Propaganda," BBC, March 31, 2025, https://monitoring.bbc.co.uk/product/b0003msc.

173 Matthew Ford, *War in the Smartphone Age: Conflict, Connectivity and the Crises at our Fingertips* (Oxford University Press, 2025); Marijn Hoijtink and Anneroos Planqué-van Hardeveld, "Machine Learning and the Platformization of the Military: A Study of Google's Machine Learning Platform TensorFlow," *International Political Sociology* 16 (2022), 1–19, https://academic.oup.com/ips/article/16/2/olab036/6562417?login=false; Sarah Grand-Clément, "Artificial Intelligence Beyond Weapons: Application and Impact of AI in the Military Domain," UNIDIR, Geneva, 2023, https://unidir.org/publication/artificial-intelligence-beyond-weapons-application-and-impact-of-ai-in-the-military-domain/; and Peter Svenmarck et al., "Possibilities and Challenges for Artificial Intelligence in Military Applications," NATO Big Data and Artificial Intelligence for Military Decision Making Specialists' Meeting Conference Paper, 2018, https://www.researchgate.net/publication/326774966_Possibilities_and_Challenges_for_Artificial_Intelligence_in_Military_Applications.

174 Kateryna Bondar, "Does Ukraine Already Have Functional CJADC2 Technology?," Center for Strategic and International Studies, December 11, 2024, https://www.csis.org/analysis/does-ukraine-already-have-functional-cjadc2-technology.

175 Joseph Clark, "Hicks Announces Delivery of Initial CJADC2 Capability," U.S. Department of War, February 21, 2024, https://www.war.gov/News/News-Stories/Article/Article/3683482/hicks-announces-delivery-of-initial-cjadc2-capability/; and "Summary of the Joint All Domain Command and Control (JADC2) Strategy," U.S. Department of Defense, March 2, 2022, https://media.defense.gov/2022/Mar/17/2002958406/-1/-1/1/SUMMARY-OF-THE-JOINT-ALL-DOMAIN-COMMAND-AND-CONTROL-STRATEGY.PDF.

176 Ford, *War in the Smartphone Age*.

177 Matthew Ford, "From Innovation to Participation: Connectivity and the Conduct of Contemporary Warfare," *International Affairs* 100, no. 4, (2024): 1531–49, https://doi.org/10.1093/ia/iiae061.

178 Matthew Ford and Andrew Hoskins, *Radical War: Data, Attention and Control in the Twenty-First Century* (Hurst Publishers, 2022), 47–80, https://doi.org/10.1093/oso/9780197656549.003.0004; and Ford, *War in the Smartphone Age*.

179 The importance of TikTok here will likely grow as the "mysteries" of its algorithm become available to U.S. big tech as part of a deal signed in Madrid in September 2025 by the United States and China. Steven Feldstein, "The TikTok Deal Is America's White Flag in the Tech War With China: Beijing Will Still Retain Considerable Influence over the U.S. Version of the App," *Foreign Policy*, September 29, 2025, https://foreignpolicy.com/2025/09/29/tik-tok-deal-tech-war-china/; John Cassidy, "Donald Trump's TikTok Deal Looks Like Crony Capitalism," *The New Yorker*, September 29, 2025, https://www.newyorker.com/news/the-financial-page/donald-trumps-tiktok-deal-looks-like-crony-capitalism; and Lauren Forristal, "Here's What's Happening Right Now with the US TikTok Deal," TechCrunch, September 26, 2025, https://techcrunch.com/2025/09/26/heres-whats-happening-right-now-with-the-us-tiktok-deal/.

180 Palantir is probably the best-known and most controversial platform for four reasons: First, the dramatic increase in its stock price since the deployment of its software by the United States (see Faizan Farooque, "The Stock Market Laughed, Then Palantir Redefined the Fight," The Street, October 6, 2025, https://www.thestreet.com/technology/the-stock-market-laughed-then-palantir-redefined-the-fight. Second, the political and financial support of Palantir's chairman (and PayPal co-founder) Peter Thiel for Trump and Vice President J.D. Vance (see Vittoria Elliott, "Tech Billionaires Already Captured the White House. They Still Want to Be Kings," *WIRED*, September 26, 2025, https://www.wired.com/story/tech-billionaires-communities/). Third, the fact that Palantir's founders, Peter Thiel and Alex Karp, have taken up and repeated the ideas of Curtis Yarvin, who some critics contend is a techno-fascist (see Luke Munn, "The Rise of 'Techno-Fascism,'" Openforum.com.au, May 18, 2025, https://www.openforum.com.au/the-rise-of-techno-fascism/). Fourth, the use of Palantir's software by the Israel Defense Forces in Gaza (see Julian Borger, "Global Firms 'Profiting from Genocide' in Gaza, Says UN Rapporteur," *Guardian*, July 3, 2025, https://www.theguardian.com/world/2025/jul/03/global-firms-profiting-israel-genocide-gaza-united-nations-rapporteur).

181 Dominika Kunertova et al., "Russian and Ukrainian Advantages in Drone Warfare," War on the Rocks, June 10, 2025, https://warontherocks.com/2025/06/in-brief-russian-and-ukrainian-advantages-in-drone-warfare/; and Mark Hvizda et al., "Dispersed, Disguised, and Degradable: The Implications of the Fighting in Ukraine for Future US-Involved Conflicts," Rand, 2015, https://www.rand.org/content/dam/rand/pubs/research_reports/RRA3100/RRA3141-2/RAND_RRA3141-2.pdf.

182 Maryanne Kelton et al., "Virtual Sovereignty? Private Internet Capital, Digital Platforms and Infrastructural Power in the United States," *International Affairs* 98, no. 6 (2022), 1977–99, https://doi.org/10.1093/ia/iiac226.

183 John A. Nagle and Katie Crombe, *A Call to Action: Lessons from Ukraine for the Future Force* (Strategic Studies Institute and US Army War College Press, 2024), xxvi.

184 General Jim Hockenhull, "How Open-Source Intelligence Has Shaped the Russia-Ukraine War," RUSI Members Webinar, December 9, 2022, https://www.gov.uk/government/speeches/how-open-source-intelligence-has-shaped-the-russia-ukraine-war.

185 Gabriella N. Boyes, Jingyuan Chen, and Vincent R. Scauzzo, "Lessons from Ukraine for the Future Force," in *A Call to Action*, ed. John A. Nagle and Katie Crombe (Strategic Studies Institute and US Army War College Press, 2024); and "The Operational Environment 2024-2034: Large Scale Combat Operations," U.S. Army, TRADOC G-2, 2024, https://oe.tradoc.army.mil/product/the-operational-environment-2024-2034-large-scale-combat-operations/.

186 On Palantir's early role soon after the war started, see Vera Bergengruen, "How Tech Giants Turned Ukraine Into an AI War Lab," *Time,* February 8, 2024, https://time.com/6691662/ai-ukraine-war-palantir/; and Daniel Kosoy, "Palantir, the Secretive Tech Giant Shaping Ukraine's Tech Effort," United 24 Media, January 31, 2025, https://united24media.com/war-in-ukraine/palantir-the-secretive-tech-giant-shaping-ukraines-war-effort-5519.

187 Sam Bresnick, Ngor Luong, and Kathleen Curlee, "Which Ties Will Bind?," Center for Security and Emerging Technology, February 2024, 54, https://cset.georgetown.edu/publication/which-ties-will-bind and Christopher Miller, Mark Scott, and Bryan Bender, "UkraineX: How Elon Musk's Space Satellites Changed the War on the Ground," Politico, June 8, 2022, https://www.politico.eu/article/elon-musk-ukraine-starlink/. Ukraine's reliance on private tech is not without its challenges, though, as the country remains beholden to actors like Elon Musk, who can decide whether to turn off SpaceX/Starlink satellite internet services if he so chooses. See Mathieu Pollet, "Ukraine Is Stuck with Musk's Starlink for Now: Key Competitor Eutelsat Won't Break Starlink's Grip on Kyiv's Wartime Communications Overnight," Politico, April 7, 2025, https://www.politico.eu/article/ukraine-stuck-with-elon-musk-starlink-satellite-internet/.

188 Bresnick, Luong, and Curlee, "Which Ties Will Bind?," 15, 53; Sam Bendett, "Roles and Implications of AI in the Russian-Ukrainian Conflict," *Russia Matters*, Harvard Kennedy School Belfer Center for Science and International Affairs, July 20, 2023, https://www.russiamatters.org/analysis/roles-and-implications-ai-russian-ukrainian-conflict; and "Get Ahead of Present and Future Attacks with Recorded Future," Recorded Future, accessed March 25, 2025, https://www.recordedfuture.com/get-ahead-of-present-and-future-attacks/.

189 Hockenhull, "How Open-Source Intelligence Has Shaped the Russia-Ukraine War."

190 Matthew Ford, "Ukraine, Participation and the Smartphone at War," *Political Anthropological Research on International Social Sciences* 4, no. 2 (2023), 219–47.

191 "How Technology Helped Ukraine Resist During Wartime," Microsoft, January 20, 2023, https://news.microsoft.com/en-cee/2023/01/20/how-technology-helped-ukraine-resist-during-wartime/.

192 The war in Gaza throws up some of the most telling examples. *+972 Magazine* and *The Guardian* report that, in September 2025, Microsoft cancelled a contract with the IDF, through which the company was storing mobile phone data for the entire Palestinian population on its cloud platform Azure. This data was being used by the IDF's Unit 8200 for "lethal airstrikes in Gaza," as well as to arrest Palestinians in the West Bank. Yuval Abraham, "Microsoft Storing Israeli Intelligence Trove Used to Attack Palestinians," *+972 Magazine*, August 6, 2025, https://www.972mag.com/microsoft-8200-intelligence-surveillance-cloud-azure/; Harry Davies and Yuval Abraham, "'A Million Calls an Hour': Israel Relying on Microsoft Cloud for Expansive Surveillance of Palestinians," *Guardian*, August 6, 2025, https://www.theguardian.com/world/2025/aug/06/microsoft-israeli-military-palestinian-phone-calls-cloud; Harry Davies and Yuval Abraham, "Microsoft Blocks Israel's Use of Its Technology in Mass Surveillance of Palestinians," *Guardian*, September 26, 2025, https://www.theguardian.com/world/2025/sep/25/microsoft-blocks-israels-use-of-its-technology-in-mass-surveillance-of-palestinians.

193 Rocco Bellanova et al., "Toward a Critique of Algorithmic Violence," *International Political Sociology* 15, 2021, 138, https://doi.org/10.1093/ips/olab003.

194 Richard Kahn, "Bot Farms: What They Are & How They're Used," Anura, November 4, 2025, https://www.anura.io/blog/what-are-bot-farms.

195 Gavin Wilde, "The Path to War Is Paved with Obscure Intentions: Signalling and Perception in the Era of AI," Just Security, October 20, 2023, https://www.justsecurity.org/89641/the-path-to-war-is-paved-with-obscure-intentions-signaling-and-perception-in-the-era-of-ai/.

196 "[DILEMA Lecture] How AI and Automation Are Making the State and War Incidental to Warfare," talk by Rupert Barrett-Taylor, November 14, 2024, posted November 15, 2024, by T.M.C. ASSER Instituut, YouTube, 49 min., 17 sec., https://www.youtube.com/watch?v=hI_V3DMkqUY.

197 Ryan McMorrow et al., "China Moves to Take 'Golden Shares' in Alibaba and Tencent Units," *Financial Times*, January 13, 2023, https://www.ft.com/content/65e60815-c5a0-4c4a-bcec-4af0f76462de; and "Who Owns ByteDance?," Canvas Business Model, October 2, 2024, https://canvasbusinessmodel.com/blogs/owners/bytedance-who-owns.

198 "TikTok: How Congress Can Safeguard American Data Privacy and Protect Children from Online Harms," U.S. House of Representatives Committee on Energy and Commerce, March 20, 2023, https://d1dth6e84htgma.cloudfront.net/Memo_03_23_2023_Full_Committee_Tik_Tok_Hearing_55e129f043.pdf?updated_at=2023-03-20T21:12:05.159Z.

199 Liv McMahon and Graham Fraser, "Trump Claims a TikTok Deal Is Done. Who Would Own It, and How Would It Work?,'" BBC News, September 30, 2025, https://www.bbc.com/news/articles/clyng762q4eo.

200 Justin Elliott and Joshua Kaplan, "Elon Musk's SpaceX Took Money Directly From Chinese Investors, Company Insider Testifies," ProPublica, October 2, 2025, https://www.propublica.org/article/elon-musk-spacex-china-investors-court-testimony?utm_source=substack&utm_medium=email.

201 Loren Thompson, "Microsoft's Big Footprint In China Is Out of Step with U.S. Security Concerns," *Forbes*, June 12, 2023, https://www.forbes.com/sites/lorenthompson/2023/06/12/microsofts-big-footprint-in-china-is-out-of-step-with-us-security-concerns/.

202 Telegeography, "Submarine Cable Map," 2Africa, September 24, 2024, https://www.submarinecablemap.com/submarine-cable/2africa.

203 Zijing Wu and Michael Acton, "Nvidia Plans Shanghai Research Centre in New Commitment to China: US Chipmaker Considers Expanding Its Presence in the Country Even as Sales Are Hit by Washington's Export Controls," *Financial Times*, May 16, 2025, https://www.ft.com/content/c886a4c0-da75-4ea7-8230-6ffd18815fa4?utm_source=substack&utm_medium=email.

204 Tripp Mickle, "Apple's A.I. Ambitions for China Provoke Washington's Resistance: The Trump Administration and Congressional Officials Have Raised Concerns About a Deal to Put a Chinese Company's Artificial Intelligence on iPhones," *New York Times*, May 17, 2025, https://www.nytimes.com/2025/05/17/technology/apple-alibaba-ai-tool-china.html?utm_source=substack&utm_medium=email.

205 Vera Bergengruen, "How Telegram Became the Digital Battlefield in the Russia-Ukraine War," *Time*, March 22, 2022, https://time.com/6158437/telegram-russia-ukraine-information-war/.

206 Sareena Dayaram, "Hong Kong's Student Protesters Catch Up on Class the Same Way They Organize: On an Encrypted Messaging App," NBC News, November 16, 2019, https://www.nbcnews.com/tech/tech-news/hong-kong-s-student-protesters-catch-class-same-way-they-n1082776.

207 "The App in the War. What Does Telegram Do for Ukraine and Russia?," elBelSat, September 6, 2024, https://en.belsat.eu/82167037/the-app-in-the-war-what-does-telegram-do-for-ukraine-and-russia; and Peter Schrijver, "Ukrainian Intelligence's Use of Telegram in Wartime," *International Journal of Intelligence and Counterintelligence,* July 8, 2025, https://www.tandfonline.com/doi/full/10.1080/08850607.2025.2522222#abstract.

208 "Ukraine Bans Officials from Using Telegram on State-Issued Devices," Al Jazeera, September 21, 2024, https://www.aljazeera.com/news/2024/9/21/ukraine-bans-officials-from-using-telegram-on-state-issued-devices.

209 "Russia Restricts WhatsApp and Telegram, Alleging Apps Used for Fraud and Terrorism," *Guardian,* August 14, 2025, https://www.theguardian.com/world/2025/aug/13/russia-clamps-down-on-whatsapp-and-telegram-over-data-sharing.

210 Bondar, "Does Ukraine Already Have Functional CJADC2 Technology?"

211 Clay Huffman, "Intelligence," in *A Call to Action*, ed. John A. Nagle and Katie Crombe (Strategic Studies Institute and U.S. Army War College Press, 2024), 82; and Vera Bergengruen and Margarita Konaev, "How Tech Giants Turned Ukraine into an AI War Lab," *Time*, February 8, 2024, https://cset.georgetown.edu/article/how-tech-giants-turned-ukraine-into-an-ai-war-lab/.

212 Jake Lahut, "The GOP's Message for Tech Billionaires: Be Like Peter Thiel," *Wired*, July 23, 2025, https://www.wired.com/story/peter-thiel-silicon-valley-billionaires-dc/.

213 Michael Sion, John Wenzel, and Blaine Pellicore, "Rethinking Defense: The Role of Private Capital," Bain & Company, December 2024, https://www.bain.com/insights/rethinking-defense-the-role-of-private-capital/.

214 "Defense Tech Investments," Sagamore Institute, July 2024, https://sagamoreinstitute.org/defense-tech-investments/.

215 Jeffrey Dastin, "Ukraine Is Using Palantir's Software for 'Targeting,'" CEO Says," Reuters, February 1, 2023, https://www.reuters.com/technology/ukraine-is-using-palantirs-software-targeting-ceo-says-2023-02-02/.

216 "Gotham: Your Software Is the Weapons System," Palantir Technologies, accessed November 24, 2025, https://www.palantir.com/platforms/gotham/; and "AI-Enabled Operations," Palantir Technologies, 2022, https://www.palantir.com/assets/xrfr7uokpv1b/3A0y10xksgXENvRMNaAsUu/ed8f7f1ed534c-0101f64536a85f7297b/Gotham_AI-Enabled_Operations_White_Paper.pdf.

217 Elke Schwarz, "From Blitzkrieg to Blitzscaling: Assessing the Impact of Venture Capital Dynamics on Military Norms," *Finance and Society* (2025), 3 and 19, https://doi.org/10.1017/fas.2024.18; and Mark Howard, "The Rapacious Ambivalence of VC Investment: Venture Capital, Value Capture, and the Valorization of Crisis," *Finance and Society* 10, no. 2 (August 2024), 91, https://doi.org/10.1017/fas.2024.1.

218 "Deadly Drones: Civilians at Risk from Short-Range Drones in Frontline Areas of Ukraine, 24 February 2022 — 30 April 2025," Human Rights Office of the High Commissioner, Accessed November 24, 2025, https://ukraine.ohchr.org/en/Deadly-drones-Civilians-at-risk-from-short-range-drones-in-frontline-areas-of-Ukraine-24-February-2022-30-April-2025; "Case Studies in Drone Warfare: Successes, Controversies, and Lessons Learned," National Defense Lab, accessed November 24, 2025, https://nationaldefenselab.com/news/details/case-studies-in-drone-warfare-successes-controversies-and-lessons-learned; and Lidia Bernd, "Precision and Peril: The Strategy and Consequences of Targeted Killings," *Georgetown Security Studies Review* (August 2025), https://gssr.georgetown.edu/the-forum/regions/mena/precision-and-peril-the-strategy-and-consequences-of-targeted-killings/.

219 Jim Garamone, "Milley Makes Case for Rules-Based Order, Deterrence in New Era," U.S. Department of Defense, June 30, 2023, https://www.war.gov/News/News-Stories/Article/Article/3446709/milley-makes-case-for-rules-based-order-deterrence-in-new-era/; "Palantir CTO Shyam Sankar Talks Geopolitical Tensions, AI and Government Web Services," posted December 1, 2023, by CNBC Television, YouTube, 5 min., 15 sec., https://www.youtube.com/watch?v=evCotCbq9v0; and Michèle Flournoy, "AI Is Already at War: How Artificial Intelligence Will Transform the Military," *Foreign Affairs,* November/December 2023, https://www.foreignaffairs.com/united-states/ai-already-war-flournoy.

Carnegie Endowment for International Peace

In a complex, changing, and increasingly contested world, the Carnegie Endowment generates strategic ideas, supports diplomacy, and trains the next generation of international scholar-practitioners to help countries and institutions take on the most difficult global problems and advance peace. With a global network of more than 170 scholars across twenty countries, Carnegie is renowned for its independent analysis of major global problems and understanding of regional contexts.

Democracy, Conflict, and Governance Program

The Democracy, Conflict, and Governance Program is a leading source of independent policy research, writing, and outreach on global democracy, conflict, and governance. It analyzes and seeks to improve international efforts to reduce democratic backsliding, mitigate conflict and violence, overcome political polarization, promote gender equality, and advance pro-democratic uses of new technologies.

CarnegieEndowment.org