A Ukrainian marine prepares to launch a first-person-view drone 12 October 2023. (Photo courtesy of the 35th Marine Brigade, Defense Forces of Ukraine)

Democratization of Irregular Warfare

Emerging Technology and the Russo-Ukrainian War

Treston Wheat, PhD
David Kirichenko

Warfare went through drastic changes over the past millennia, but a consistent theme throughout these changes has been the increasing democratization of conflict. What was once chivalric orders gave way to mercenaries and militias, and then Napoleon Bonaparte radically altered war by raising popular armies not bound by the same hierarchical requirements as other militaries. The nineteenth and twentieth centuries saw mass mobilization through the draft, and the citizen-soldier became a critical symbol of militaries in republics and democracies. During World War II, people normally disenfranchised from society and politics were even included in the war effort, such as women taking a far more active role than ever before in conflict.[1] The history of war over the past five hundred years includes the further democratization of military power. Today, technological development has furthered democratization to a level never seen before because weapons of war like drones and cyber capabilities are available to the masses at an extremely low cost as a barrier to entry.

Russia's invasion of Ukraine provides a useful case study in how democratization has happened in three critical areas of modern warfare: drones, cyberattacks, and influence operations. The availability of the technology for regular citizens to participate in warfare has changed the way conflicts are fought, and Ukrainian citizens have demonstrated mechanisms that citizens of other countries can utilize in their own conflicts. This aspect of war is important for government analysts and scholars to understand because wars of the future are extremely likely to include this element. For example, should the United States ever go to war with China over Taiwan, netizens will likely spend an extraordinary amount of time on cyberspace defending their country's online and physical infrastructure. The Russo-Ukrainian War provides an ongoing natural experiment in how democratization of warfare is taking place, which will allow scholarship to develop concerning this novel approach to war.

Treston Wheat, PhD, is an intelligence research specialist with Insight Forward, a special advisor for geopolitics with Riley Risk, editor in chief of *The Close Protection and Security Journal* at the International Protective Security Board, and an adjunct professor at Georgetown University.

David Kirichenko is an Associate Research Fellow at the Henry Jackson Society. His work on warfare has been featured in the Atlantic Council, Center for European Policy Analysis, and *The Economist*, among many others.

Crowdsourcing Drones Supplies

Civilian funding of the military is not new to warfare (beyond the normal taxes as well). A significant portion of the American Revolution was funded through the confiscation of property, and average citizens would buy bonds to raise money for the war effort during World War II. However, the Russo-Ukrainian War has shown a different side of this kind of funding as citizens and supporters are directly buying military equipment for the soldiers on the front lines. In modern parlance, people are crowdfunding the war in Ukraine, which shows a novel way that warfare is unfolding and the aspect of the democratization of irregular war.

Lt. Col. Pavlo Kurylenko, a top Ukrainian military commander, said, "We're only holding back the Russians with crowdfunded drones."[2] He further mentioned that 90 percent of first-person view (FPV) supplies are provided by volunteers or military divisions themselves. With drones in such short supply, demand far outstrips supply. It is quickly becoming a battle of drones, and many Ukrainian units on the front line are dependent on volunteers who bring them drones.[3] Volunteer organizations like Dzyga's Paw have not only built military tech supply chains for Ukrainian units but were also at the forefront of driving drone operations innovation at the start of the war.[4] A soldier using an FPV drone can effectively neutralize heavy armor worth millions of dollars with a drone that costs just $300.[5] FPV drones equipped with cameras transmit live video to goggles or screens, letting pilots navigate via the drone's perspective. Primarily used as kamikaze drones with explosive payloads, they provide detailed views crucial for tasks demanding precision and swift pilot responses.

Paul Lushenko of the U.S. Army War College notes that drones have given "asymmetric advantages to the militaries of lesser states."[6] Drones have been so effective in warfare that Ukraine had to sideline the U.S. Abrams tanks because drones have been too effective

First-person-view drones are ready for transfer to the Ukrainian military in September 2024 as part of the Birds of Victory project. Lt. Col. Pavlo Kurylenko, a top Ukrainian military commander, said that more than 90 percent of these drones are supplied by volunteers or the military units themselves. (Photo courtesy of the Lviv Regional Military Administration)

at spotting tanks and hitting them.[7] Soldiers and heavy armor simply can't move around on the battlefield anymore without being spotted. The security world has been concerned about the ubiquity and cheapness of drones for some time, but the Russo-Ukrainian War shows the advantages in irregular warfare of this technology. Russia has significantly more manpower and resources than Ukraine. However, in typical irregular warfare, the weaker side can use novel technologies (or older technology that is adaptable) to outmaneuver the more advanced forces.

Ukraine relies not only on volunteers to source drones for the military but to also drive innovation and production of drones.[8] Numerous volunteers work in garage-style shops to make improvements to drones and are even setting up repair shops near the front line. If soldiers retrieve a damaged drone, they send it to volunteer organizations who help repair the drones for soldiers.[9] Ukrainian charities run supply chains to source drones for soldiers to help them on the battlefield.[10] Drones not only have changed the battlefield in Ukraine, but democratization has also occurred through the fact that all sorts of individuals and organizations are able to get their hands on amateur drones that anyone can buy and then supply them directly to the front.

An ability to supply conflicts more directly will majorly alter warfare as great powers could find themselves at the mercy of crowdfunded militias and guerillas. Although that itself is not necessarily new as diasporas (e.g., the Irish Republican Army) supplied irregular operations through donations.[11] What is new is the ability to buy cheap arms and bring them directly to the soldiers. Importantly, emerging technology like drones is relatively cheap. Previously, weapons systems were extraordinarily expensive, and even donations from the diaspora could only supply limited arms. Drones, on the other hand, can be supplied more easily with only a few hundred dollars. These cheap drones, which previously people could buy off the store shelves, have the ability to neutralize tanks worth millions of dollars and have made tanks play more of a secondary role in the Russo-Ukrainian War.[12] As military strategies are considering the future of irregular warfare, they will need to consider this kind of crowdsourcing from either the diaspora or supportive citizens. There

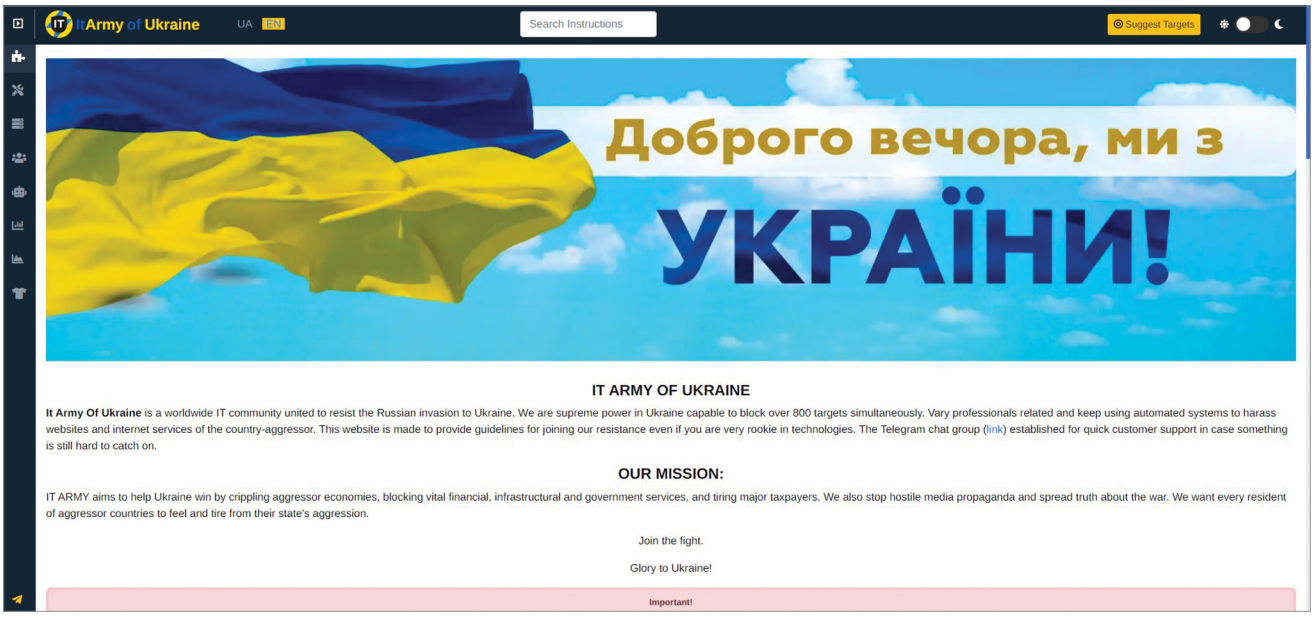
A North Atlantic Fella Organization (NAFO) mascot is perched on a destroyed Russian tank in front of the Russian embassy in Berlin on 24 February 2023. NAFO, a play on NATO, is an internet meme and social media movement dedicated to countering Russian propaganda and disinformation about the 2022 Russian invasion of Ukraine. It has been categorized as a form of information warfare. (Photo by Leonhard Lnez via Wikimedia Commons)

will need to be legal considerations for governments to work through as well. Supplying terrorist organizations (when they are officially designated as such) is illegal in Western countries, and geoeconomic considerations will need to take place. In addition, there will be security concerns even when crowdsourcing technology like drones for militaries and militias that are supported by Western governments. For example, drones made by Chinese manufacturers could have intentional vulnerabilities that leak data back to the enemy.

Cyber Operations through a Volunteer Force

Russia's full-scale invasion of Ukraine in February 2022 unleashed the first all-out cyberwar between two nation-states.[13] Many feared that Ukraine would suffer from a "digital Pearl Harbor," but that moment never came. Russian cyberattacks fizzled out, and Ukraine withstood Russia's cyber onslaught with help from both public and private partnerships from the West.[14] Ukraine also acted by going on the cyber offensive. Ukraine's Ministry of Digital Transformation spearheaded an effort to bootstrap an IT army to ensure maximum resistance.[15] Volunteer hackers from around the world joined in on the efforts to wage cyberwar alongside Ukraine's government. This IT Army of Ukraine has contributed extensively to Ukraine's cyber offensive against Russia, executing a diverse and effective range of attacks.[16] These include leaking documents from Russia's central bank, disrupting internet services in Russian-occupied territories, incapacitating one of Moscow's major internet providers, and targeting private corporations to hinder economic activities.[17]

At its peak, the group had several hundred thousand members, but the overall subscriber count and the associated impact need to be more accurate. While subscriber counts have decreased on its Telegram channel, the IT Army's attacks have grown in effectiveness



The IT Army of Ukraine has contributed extensively to Ukraine's cyber offensive against Russia. The group, at its peak, had several hundred thousand members who participated in thousands of distributed denial of service attacks throughout Russia. (Screenshot from the IT Army of Ukraine)

and scale. The primary tactic of the IT Army involves executing distributed denial of service (DDoS) attacks as it's easier than targeted cyberattacks. This approach is simple yet effective; it consists of coordinating a large number of computers to launch a concerted attack on a specific network or website. By flooding the target with an overwhelming volume of requests, the strategy aims to overload the system, ultimately causing it to crash.

According to assessments by the IT Army, the group has inflicted economic losses on Russia estimated to be between $1 billion and $2 billion.[18] Consequently, the cyberwarfare conducted by the IT Army represents a novel and innovative form of sanctions against their adversaries. Ted, the spokesperson for the IT Army of Ukraine, shared that cyber warfare can "operate as a form of economic sanction, a tool to strategically weaken an adversary's economy: the faster these digital capabilities are deployed, the more immediate the impact on the enemy's fighting capabilities."[19] In fact, the IT Army even caught the attention of officials from the Security Council of the Russian Federation.[20] One Russian official threatened Western officials, saying that by "supporting the IT ARMY, they are opening Pandora's box which will eventually turn against its masters."[21]

The IT Army's campaign against Russian internet providers led to a disruption of 40 percent of its resources at one point, leading to extensive disruptions in service.[22] *Kommersant*, a Russian daily newspaper, wrote that the "number of DDoS attacks on Russian companies doubled year on year in the first quarter. Mostly companies from critical industries ... Roskomnadzor speaks of repelling almost three times more attacks in the first quarter alone than in the entire 2023."[23] Furthermore, while Russia has invested billions of dollars in its building out its own satellite internet network, Ukraine's IT Army launched an attack in April 2024 that took out "two of the largest providers, Astra and Allegrosky," for several days.[24]

However, assembling a volunteer IT army presents a significant challenge because it introduces civilians to uncharted waters. As the world continues to digitize, there are increasing opportunities for ordinary individuals to participate in cyberwarfare when their nation's needs become apparent. This involvement helps to decentralize key aspects of warfare, showing how wars will increasingly be fought in the digital age. Ukraine has been attempting to draft legislation to provide a more formal legal structure to the fairly informal IT Army.[25] If the Ukrainian legislation in formalizing the "IT Army" is enacted, foreign volunteers seeking legal protection for participating in hacking on Ukraine's behalf would need to join Ukraine's cyber reserves. Vasileios Karagiannopoulos, an associate professor in cybercrime and cybersecurity at the University of

Portsmouth, believes that if the IT Army were incorporated into Ukraine's cyber reserves, it could help offer legal protections for civilians participating in cyberwar by offering "legal protection as combatants and potentially shield them from prosecution for their actions during the war."[26]

Importantly, not all preparations will need to be technical. One limitation that the IT Army has faced is engaging with nontechnical audiences. To scale the work of effective botnets and DDoS attacks, more people are needed to join the attacks. The average civilian citizen, though, does not consider themselves capable of conducting cyberattacks against an enemy. The reality is that anyone can follow simple instructions to download a tool and allow their computer's processing power and internet access to be added to the botnet and help flood an enemy's networks to bring them down. The IT Army also said that their cyber operations were conducted in support of bringing down Russian CCTV cameras to reduce visibility on Ukrainian drones bombing Russian oil refineries inside Russia demonstrating the ability of volunteer forces to bolster the regular military in cyberspace.[27] If there is a battlefield objective and the military needs some target to be shut down, they can relay the request to the hacker army to initiate an attack to help provide support. An easy example would be Ukraine's hacker army attacking Russian satellite systems or attacking Russian telecom providers in occupied territories, which they have previously done.

As society moves deeper into the digital age, the involvement of ordinary people in warfare will increasingly expand. Also, as economies and vital services become more integrated with the digital realm, vulnerabilities will multiply, presenting new opportunities for attacks. Countries like Taiwan and other democracies under threat should accept this reality and will need to prepare for how its citizenry will engage in cyberwar. Some military theorists have developed the idea of "cyber militias" in which private citizens could be called up or be prepared during a major cyberattack.[28] There will be a number of ways that governments can organize citizens to volunteer for service without having to join the military to contribute to the war effort.

Comparably to other aspects of democratization, there are risks from this occurring. Cyberattacks cannot always be contained, even when performed by highly professional hackers. For example, the NotPetya attack committed by a Russian threat actor spread far beyond Ukraine and devastated companies like Maersk.[29] That connection to the corporate world raises a separate issue. The democratization of cyberwar will not just involve hacktivists and citizens. Within the Russo-Ukrainian War, major technology companies have also directly participated, such as Microsoft providing intelligence on cyber incidents and SpaceX providing internet access.[30] Democratization of cyberwar means that organizations, some even powerful and well-funded, can also directly intervene in the conflict based on economic, security, or ideological interests. That will further change the nature of warfare and complicate the democratization of conflict as companies could stop hacktivists or oppose government interests as well.

Influence Operations and Social Media

When pundits think about the weaponization of social media, they usually refer to the use of social media to drive political change like the Arab Spring or how Russia used it to try and influence U.S. elections. However, use of social media and open-source intelligence can be used by nation-states to try to influence outcomes on the battlefield itself. Such information operations have been a critical part of warfare for some time, but social media now allows average citizens (even those not party to the conflict) to impact operational capabilities. The purpose of information operations is to gather relevant information on the enemy along with disseminating propaganda (white, black, and gray) to create an advantage in the war. White propaganda is truthful information shared to counter opposing narratives, black propaganda is false, distorted, or exaggerated information (i.e., disinformation), and gray propaganda is a combination of white and black.[31]

Social media is now quintessential to information operations for gathering intelligence and spreading propaganda. For example, militaries and intelligence agencies scout and extract as much information from social media and open-source intelligence to try and direct battlefield strikes. Ukrainian citizens in particular have been prolific at leveraging these tools to gather intelligence and direct attacks. For example, Russian soldiers have been tricked into revealing sensitive

The "Ghost of Kyiv" is the nickname given to a mythical MiG-29 Fulcrum flying ace credited with shooting down six Russian planes over Kyiv on 24 February 2022. The Ghost of Kyiv has been lauded as a morale booster for Ukrainians during the Russo-Ukrainian War. (Artwork by Andriy Dankovych via Wikimedia Commons)

information via Tinder.[32] Some disclosed their tactical locations through profile images while searching for companionship. One clever woman used dual Tinder accounts with varied border locations to pinpoint and report over seventy such profiles to Ukrainian authorities. Ukrainian hackers also created fake profiles on platforms like Telegram to lure Russian soldiers near Melitopol into sharing on-duty photos.[33] These images helped locate a Russian military base, leading to a targeted Ukrainian military strike days later. In August 2022, a local pro-Russian journalist shared photos online and unintentionally compromised the location of their base.[34] Shortly after, Ukraine struck the base with rockets. The journalist had shared images on Telegram that included visible details sufficient to pinpoint the Wagner base's precise location.

Similarly, messaging apps have allowed Ukrainians to spread malicious software under the guise of support. On Russian Navy Day in July 2023, Ukrainian hackers targeted Russian sailors by sending videos with deceptive "good wishes" via messaging apps. These videos, which showed Ukrainian attacks on Russian ships, contained malware that breached the sailors' phones, extracting confidential data for Ukrainian use. Many sailors thanked the senders before realizing the videos' true intent.

When it comes to propaganda, the Russo-Ukrainian War has been called the world's first TikTok war.[35] It is important to point out that Russia has used social media at a high level to try to direct the outcome of the entire war, but Ukrainians have fought back with their own information operations. Social media helps Ukraine in "crowdsourcing people to fight, materials, donations through cryptocurrencies, and more."[36] Part of that is those in the Ukrainian diaspora sharing their own perspectives, videos, and memes about

the atrocities Russia is committing. There is no clear evidence if this democratized propaganda is impactful, but that it is still occurring with regular frequency.

Then there is the issue of artificial intelligence (AI) employed in information operations. Large language models are still nascent in this area, and it remains unclear how they can effectively be utilized to gather information or spread propaganda. While North Korean hackers have been using AI tools like ChatGPT to conduct sophisticated attacks, there is no doubt that nation-states will use a tool like ChatGPT to influence the battlefield. For example, like in the case of fake Tinder women reaching out to Russian soldiers and extracting important intelligence, if either side can identify low-level soldiers on the battlefield, they can use AI to build a dossier or a profile on an individual and more easily trick them into revealing information. Researchers from the Alan Turing Institute used AI agents to collect open-source intelligence on a specified target, and then the system was able to build a "dossier on an individual and permit users to ask questions about them."[37]

The battlefield has expanded beyond the physical landscape to encompass the extensive, interconnected domain of the internet, where every click or post can have as much impact as a conventional military operation. Western military planners should understand that the next compromised service member could be a NATO soldier who accidentally leaks vital information on social media to our adversaries or falls prey to virtual "honey traps."[38] With the growing digitization of societies, these types of social media attacks will only increase in the future.

There are risks that come with the democratization of propaganda, though, and countries will have to be considerate of how supporters might cause reputational risks. Governments cannot control the kind of memes and videos that will be shared online, and it is entirely plausible that citizens will spread misinformation, disinformation, and ideologically extreme statements. Should that happen, this could harm the overall war effort by reducing broader support for the conflict. In addition, citizens participating in propaganda can plausibly lead to the spread of conspiracy theories that similarly harm support for particular operations. Social media now allows average citizens to contribute to the war effort by encouraging support, but that support can be a double-edged sword if they stray too far from the messaging or cause false beliefs to spread that turn away public support.

Conclusion

The Russo-Ukrainian War is the best-case study of modern warfare in a number of areas, and one area that will need serious analysis and scholarship is the further democratization of conflict. This article looked at the three major areas that is happening: drones, cyberattacks, and information operations. Drones are incredibly cheap to produce and purchase, and supporters of Ukraine fund them to bring them into the conflict with exceptional ease. In the cyber domain, Ukraine was able to raise a cyber militia to support attacks against Russia and bolster the defense of the homeland. Then on social media, netizens and global supporters help shape the narrative of the conflict while also gathering critical information on Russian soldiers and operations. Each of these areas shows how regular citizens can far more easily participate in warfare to support their countries, but the war is ongoing. Further scholarship will be needed to explore this phenomenon more fully.

However, governments and military strategists can already learn a tremendous amount from the information currently available. In bygone decades, militias would serve the purpose of bringing regular citizens into war. The American Revolution was only successful because of the many militias that supported the regular military. Now, military leaders will need to strategize on how to incorporate regular citizens in new and different ways. Could they create a coordinated propaganda campaign using netizens to spread videos and memes to turn a population against its government? Can they create "cyber militias" where patriotic hackers become part of the reserves and called up to attack foreign enemies? Are drones and other cheap technology the new "war bonds" that would allow people to give resources to the war effort? These are only the start of the questions military and government leaders will need to ask when creating strategies for the future of war.

The great war theorist Carl von Clausewitz articulated in his writings the nature of "small wars." For Clausewitz, a small war included irregular units that supported the regular army in the field by gathering

intelligence and guerilla attacks on the enemy (what was then called partisan warfare). In *On War*, Clausewitz spends time on this concept while discussing general uprisings, and he notes that the system of conscription and militias "run in the same direction when viewed from the standpoint of the older, narrower military system, and that also leads to the calling out of the home guard and arming the people."[39] Of course, he was referring to physically arming the people to support the military through irregular operations, but his concept remains valid for the new democratization efforts that are far more extensive. Rather than armed citizens attacking foreign militaries on the battlefield, "armed" citizens are fighting with propaganda on social media, using cheap drones, and engaging in cyberattacks against the enemy's critical infrastructure. The democratization of warfare is not a new concept and has been part of the broader trends of conflict for centuries, but the Russo-Ukrainian War shows how technology has furthered that democratization and how it will differ in wars of the future. ■

Notes

1. Williamson Murray and Allan Millett, *A War to Be Won: Fighting the Second World War* (Cambridge, MA: Belknap Press, 2001), 550–53.

2. David Knowles, "'We're Only Holding Back the Russians with Crowdfunded Drones,' Says Ukraine Commander," *Telegraph* (website), 12 April 2024, https://www.telegraph.co.uk/world-news/2024/04/12/only-crowdfunded-drones-holding-the-russians-back-ukraine/.

3. David Kirichenko, "A War for the Soul of Humanity," Ukrainian Research Institute, 7 December 2023, https://war.huri.harvard.edu/2023/12/07/a-war-for-the-soul-of-humanity/.

4. David Kirichenko, "How Geeks of War Mobilized Ukraine Drone Operations," Asia Times, 19 July 2024, https://asiatimes.com/2024/07/how-geeks-of-war-mobilized-ukraine-drone-operations.

5. David Kirichenko, "Drone Arms Race on Battlefield Ukraine," *Kyiv Post* (website), 7 January 2024, https://www.kyivpost.com/post/26425.

6. Ibid.

7. Sally Guyoncourt, "Why Tanks on Both Sides Are Being Sidelined on Ukraine's Battlefields," iNews, 27 April 2024, https://inews.co.uk/news/world/ukraine-us-tanks-russia-drones-3025730.

8. Alya Shandra, "Inside Ukraine's Secret FPV Drone Labs Racing to Stay Ahead of Russia," Euromaidan Press, 25 January 2024, https://euromaidanpress.com/2024/01/25/how-fpv-drones-became-ukraine-top-weapon/.

9. David Kirichenko, "Ukraine Now Has Drones Rescuing Fallen Drones from Hazardous Battlefields," Euromaidan Press, 7 May 2024, https://euromaidanpress.com/2024/05/07/ukraine-now-has-drones-rescuing-fallen-drones-from-hazardous-battlefields/.

10. Volodymyr Hrebeniuk, Andrii Bobak, and Taras Paslavskyi, "How Ukrainian Charity Foundations Purchased Drones," Vox Ukraine, 27 February 2024, https://voxukraine.org/en/how-ukrainian-charity-foundations-purchased-drones.

11. Ed Moloney, *A Secret History of the IRA* (New York: W. W. Norton, 2003), 460.

12. David Kirichenko, "The Era of the Cautious Tank," Center for European Policy Analysis, 13 September 2024, https://cepa.org/article/the-era-of-the-cautious-tank/.

13. David Kirichenko, "Lessons from the First Cyberwar: How Supporting Ukraine on the Digital Battlefield Can Help Improve the UK's Online Resilience," Henry Jackson Society, 20 February 2024, https://henryjacksonsociety.org/publications/lessons-from-the-first-cyberwar-how-supporting-ukraine-on-the-digital-battlefield-can-help-improve-the-uks-online-resilience/.

14. Ibid.

15. Matt Burgess, "Ukraine's Volunteer 'IT Army' Is Hacking in Uncharted Territory," Wired, 27 February 2022, https://www.wired.com/story/ukraine-it-army-russia-war-cyberattacks-ddos/.

16. David Kirichenko, "Ukraine's Volunteer IT Army Confronts Tech, Legal Challenges," Center for European Policy Analysis, 27 November 2023, https://cepa.org/article/ukraine-volunteer-it-army-confronts-tech-legal-challenges/.

17. David Kirichenko, "Ukraine's IT Hacker Army Requires a Non-Technical Solution to Scale," *New Eastern Europe* (website), 19 July 2024, https://neweasterneurope.eu/2024/07/19/ukraines-it-hacker-army-requires-a-non-technical-solution-to-scale/.

18. David Kirichenko, "How Ukraine Built a Volunteer Hacker Army from Scratch," Euromaidan Press, 16 January 2024, https://euromaidanpress.com/2024/01/16/how-ukraine-built-a-volunteer-hacker-army-from-scratch/.

19. Ibid.

20. Ivan Egorov, "Russian Security Council: Ukrainian Hackers from the 'IT Army' Are Recruited and Trained in the Baltic Countries [in Russian]," *Rossiyskaya Gazeta* (website), 5 March 2024, https://rg.ru/2024/03/05/sovbez-rf-ukrainskih-hakerov-iz-it-armii-verbuiut-i-gotoviat-v-stranah-baltii.html.

21. Ibid.

22. Roman Rozhkov, "DDoS to Every Home: How Hackers Attack Operators and Energy Sales Companies in the Regions [in Russian]," *Forbes* (website), 12 February 2024, https://www.forbes.ru/tekhnologii/505933-ddos-v-kazdyj-dom-kak-hakery-atakuut-operatorov-i-energosbytovye-kompanii-v-regionah.

23. "Hackers Went According to Distribution [in Russian]," *Kommersant* (website), April 2024, https://www.kommersant.ru/doc/6649341.

24. Anna Ustinova, "Putin Promised to Allocate 116 Billion Rubles for Satellite Internet [in Russian]," *Vedomosti* (website), 1 March 2024, https://www.vedomosti.ru/technology/articles/2024/03/01/1023124-putin-poobeschal-videl-it-na-sputnikovii-internet-116-mlrd-rublei.

25. Shaun Waterman, "Ukraine Scrambles to Draft Cyber Law, Legalizing Its Volunteer Hacker Army," *Newsweek* (website), 14 March 2023, https://www.newsweek.com/

ukraine-drafting-new-law-legalizing-volunteer-hacker-cyber-army-red-cross-1786814.

26. Kirichenko, "How Ukraine Built a Volunteer Hacker Army from Scratch."

27. David Kirichenko, "Ukraine's IT Army Now Aids Drone Strikes on Russian Oil Refineries," Euromaidan Press, 29 June 2024, https://euromaidanpress.com/2024/06/29/ukraines-it-army-now-aids-drone-strikes-on-russian-oil-refineries/.

28. Dan Jerker B. Svantesson, "Regulating a 'Cyber Militia' – Some Lessons from Ukraine, and Thoughts about the Future," *The Scandinavian Journal of Military Studies* (website), accessed 28 October 2024, https://sjms.nu/articles/10.31374/sjms.195.

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

30. Treston Wheat, *"A State in Disguise of a Merchant": Multinational Tech Corporations and Reconfiguration of the Balance of Power in Asia* (Jaffrey, NH: Andrew W. Marshall Foundation, October 2022), https://www.andrewwmarshallfoundation.org/library/a-state-in-disguise-of-a-merchant-multinational-tech-corporations-and-the-reconfiguration-of-the-balance-of-power-in-asia/.

31. Loch K. Johnson, *The Third Option: Covert Action and American Foreign Policy* (New York: Oxford University Press, 2022), 23–24.

32. Jesse O'Neill, "'Sleeping with the Enemy' Russian Troops Try to Pick Up Ukrainian Women on Tinder," *New York Post* (website), 24 February 2022, https://nypost.com/2022/02/24/ukrainian-women-say-russian-troops-are-flirting-with-them-on-tinder/.

33. Mehul Srivastava, "Ukraine's Hackers: An Ex-Spook, a Starlink and 'Owning' Russia," *Financial Times* (website), 3 September 2022, https://www.ft.com/content/f4d25ba0-545f-4fad-9d91-5564b4a31d77.

34. Matt Burgess, "Their Photos Were Posted Online. Then They Were Bombed," *Wired* (website), 26 August 2022, https://www.wired.com/story/wagner-group-osint-russia-ukraine/.

35. Kyle Chayka, "Watching the World's 'First TikTok War,'" *New Yorker* (website), 3 March 2022, https://www.newyorker.com/culture/infinite-scroll/watching-the-worlds-first-tiktok-war.

36. Sara Brown, "In Russia-Ukraine War, Social Media Stokes Ingenuity, Disinformation," MIT Sloan School of Management, 6 April 2022, https://mitsloan.mit.edu/ideas-made-to-matter/russia-ukraine-war-social-media-stokes-ingenuity-disinformation.

37. Ardi Janjeva et al., *The Rapid Rise of Generative AI Assessing Risks to Safety and Security* (London: Centre for Emerging Technology and Security, December 2023), https://cetas.turing.ac.uk/sites/default/files/2023-12/cetas_research_report_-_the_rapid_rise_of_generative_ai_-_2023.pdf.

38. David Kirichenko, "The Growing Use of Scamming Techniques and Social Media on the Battlefield," Irregular Warfare Center, 18 October 2023, https://irregularwarfarecenter.org/publications/perspectives/the-growing-use-of-scamming-techniques-and-social-media-on-the-battlefield/.

39. Carl von Clausewitz, *On War*, trans. Michael Howard and Peter Paret (New York: Oxford University Press, 2007), 184.