The Ukrainian Information and Cyber War

Chris Bronk
Gabriel Collins
Dan S. Wallach

ABSTRACT

Information and cyber action have been important but ancillary components of the Ukraine war since its outbreak on February 24, 2022. We offer a set of observations:

- *A form of cyber conflict has emerged in which Russia often attempts to aggressively deny service or purloin information, while Ukraine and its allies often blunt the attacks;*
- *Communications security for Russian forces from the tactical- to theater-level has frequently failed, often with disastrous consequences, as signals intelligence information has been employed to target military command echelons;*
- *Unmanned aircraft have come to occupy a critical intelligence and air support function for Ukraine, although Russia is increasingly able to employ drones as well;*
- *Intelligence support from the West to Ukraine appears highly significant and useful, possibly substantially shaping Ukrainian strategy and tactics;*
- *The infrastructure and technical expertise of large tech firms such as Google, Microsoft, and SpaceX also helped Ukraine stay abreast of the Russian cyber threats; and*
- *Propaganda operations by Ukraine have had tremendous reach in Europe and continue to elicit support, while those of Russia have been largely inward-facing and designed to shore up support for the war among the Russian public.*

We also consider what cyber tools and effects might be employed as the war continues.

Chris Bronk is an associate professor with tenure, in the Hobby School of Public Affairs at the University of Houston. An academic-practitioner with manifold interests, he directed UH's graduate cybersecurity program and was faculty in the College of Technology. Bronk publishes interdisciplinary research at the intersection of technology and policy, frequently in collaboration with undergraduate and graduate students. He published a book, Cyber Threat: The Rise of Information Geopolitics in U.S. National Security and has engaged in scholarship on Internet censorship, online surveillance, border security, public diplomacy, organization information technology, and critical infrastructure protection. His academic work has been sponsored by the National Science Foundation, Department of Energy, Department of Defense, Department of Homeland Security, Deloitte, Microsoft, and AT&T. He has served as both a Foreign Service Officer and Senior Advisor at the U.S. Department of State, managing the deployment of its enterprise wiki, Diplopedia, which remains in use today.

INTRODUCTION

In a matter of months the Ukraine war will enter its third year.[1] At the outset of hostilities, many figured that Moscow's bold gamble to storm Ukraine by force and seize the country's capital would succeed as similar operations did in Hungary (1956), Czechoslovakia (1968), and Afghanistan (1979). Before this invasion commenced, no one knew how effectively Ukraine's military would fight. Once the shooting started, we learned that Ukraine's military was indeed motivated and fought well. With the war now marked by several major shifts on the battlefield, we believe it is wise to consider less tangible forms of action that have occurred, and how they may shape future fighting. There have been some real surprises in this war including in cyber and information operations. An accounting of both is provided here, as well as how information and cyber action may influence the outcome of this war, whether it ends in a negotiated settlement, capitulation, or collapse.

The unexpected turns of the Ukraine war have yielded observations that cover communications, logistics, operational art, and a variety of other topics, including information and computation. From propaganda to air defense, this war is one in which the proliferation of computation and information technologies has produced a battlefield environment vastly different from earlier conventional engagements of the post-Cold War period. We will cover a range of issues, some more briefly than others, and we obviously are unaware of the classified operations undertaken by the belligerents and their supporters. Early on, we saw publicly reported snippets alluding to US information sharing,[2] and of Chinese cyber operations supporting Russia,[3] and other reports over time that suggest that the information battle is often as surprising as the kinetic conflict.

Gabriel Collins is the Baker Botts Fellow in Energy and Environmental Regulatory Affairs at Rice University's Baker Institute for Public Policy's Center for Energy Studies and a Senior Visiting Research Fellow at the Oxford Institute for Energy Studies. At Baker, he co-heads the Program on Energy & Geopolitics in Eurasia. Gabe's research portfolio covers a range of energy, water, and national security issues. Collins received his B.A. from Princeton University and a J.D. from the University of Michigan Law School. He was a member of the China Maritime Studies Institute team, is still teased by his family for joining a commodity hedge fund in 2008, has practiced law, and is now thrilled to be at the premier global energy & resource think-tank. Gabe is a Permian Basin native, reads Mandarin and Russian well enough to use them in his research, speaks each just well enough to get himself in trouble, and is licensed to practice law in Texas.

THE CYBERS

Many observers were surprised when hostilities commenced at the absence of a crippling cyberattack on the Ukrainian telecommunications infrastructure. In the earliest hours of fighting, the world watched as armored columns streamed by Ukrainian border checkpoint cameras that passed their images over the internet unimpeded. Ukraine stayed online as Russia invaded. Both Russian and US military doctrine now include the use of cyber effects alongside traditional "kinetic" warfare. We know the Russians tried to cause cyber effects, including Russian attacks on ViaSat 's modems,[4] which were mitigated by new connectivity via SpaceX's StarLink orbital information network. Subsequent Russian attacks on StarLink were unsuccessful.[5] Efforts notwithstanding, as of the date of this article, Russia has failed to close off Ukraine from cyberspace.

The failure of Russia's early-on cyber operations clearly played in Ukraine's favor, with Ukraine maintaining both internal communications and the wherewithal to disseminate to the world, whether through traditional news channels or through YouTube, TikTok, and other online forms of media. Also, while we would not know until later, the US had established secure communications from Ukraine to the US military's European Command.[6]

A related surprise was the absence of effects from massive cyberattacks aimed at Ukraine's critical infrastructure. In 2015 and again in 2016, Russia conducted against Ukraine some of the cleverest hacks of electricity infrastructure seen anywhere heretofore.[7] A year later, Russia launched Petya/NotPetya, a massively destructive set of false ransomware attacks against Ukrainian government and commercial targets. Petya had a far-reaching impact on firms beyond Ukraine as well, which was severely destructive of international cargo carrier Maersk.[8] We have yet to see this magnitude of destructive cyberattack against Ukraine, possibly because such attacks were thwarted, or because of rapid repair.

Dan S. Wallach is a Professor in the Departments of Computer Science and Electrical and Computer Engineering and a Rice Scholar at the Baker Institute for Public Policy at Rice University in Houston, Texas. His research considers a variety of computer security topics, including electronic voting, Internet censorship, and security issues in web browsers, servers, and smartphone applications. Wallach served on the Air Force Science Advisory Board (2011-2015) and as a member of the U.S. Election Assistance Commission's Technical Guidelines Development Committee (2019+). He will soon be on leave from Rice to serve as a DARPA program manager.

Before the war, there was an assumption that cyber action would be at the center of any Russian kinetic campaign.[9] This was the case when Russia attacked Georgia in 2008. But now we proffer a new hypothesis: that Russia went for broke with cyber action in its earlier campaigns in Ukraine (2012) and in Syria (2015). Lessons learned (by Ukraine and others) have been applied in Ukraine in 2022, blunting the impact of more recent cyberattacks. For example, IBM's Security X-Force group has documented "at least six" Russian campaigns targeting Ukraine and has published a list of security indicators to help thwart them. Of course, there have been many other documented cyberattacks, both before and after the invasion began.[10] This suggests that cyber's role in Russian military planning is a form of "icing on the cake." It is nice to have, but hardly a prerequisite for launching a kinetic attack.

In addition, there is ample evidence that the global IT industry in general, and Ukraine's IT community in particular, has been better prepared for destructive Russian cyberattacks than before. Nonetheless, Microsoft asserts with a great degree of confidence that during this war Russia has launched "destructive cyberattacks within Ukraine, network penetration and espionage outside Ukraine, and cyber influence operations targeting people around the world."[11] While some experts feel Microsoft's claims are overblown,[12] the pattern of cyberattacks against Ukraine being discovered and mitigated seems clear. The Defense Department's U.S. Cyber Command (USCYBERCOM) made contributions by releasing cyber indicators of compromise valuable to the Ukrainians and available by Pastebin to all.[13]

At the one-year mark in fighting, summaries on the cyber conflict by two of the United States's largest IT companies, Microsoft, and Google (through its Mandiant subsidiary) showed a more nuanced picture. Both firms actively support cyber defense actions to protect Ukrainian information resources as well as those of nations actively supporting the Ukrainians. These companies generate a massive amount of data regarding malicious activity in cyberspace. Google's visibility into cybersecurity matters was greatly augmented when it acquired Mandiant, a dominant commercial response and intelligence entity. Microsoft, with its massive global software install base also enjoys unique visibility in the Ukraine war's cyber conflict. Their assessments both deserve attention.

Google collected and confirmed a 250 percent increase in "phishing" email activity designed to compromise Ukraine's computer systems and a 300 percent increase in NATO member states.[14] Destructive cyber activity by Russian GRU (military intelligence) operatives have largely been confined to "wiper" attacks designed to delete data as well as cryptographic ransomware ones that deny data access. Interestingly, there has not been a major spillover of destructive malware outside of Ukraine as occurred with GRU's 2017 *NotPetya* campaign.[15]

Microsoft's report at the one-year mark similarly assesses Russia's cyber operations, pointing the finger at Russia for a "ransomware operation against the transportation sector in Poland, a NATO member and key logistical hub for Ukraine-bound supplies." In addition to destructive cyber activity, Microsoft states that the GRU, "potentially compromised a separate Polish transportation sector firm, and later increased reconnaissance against NATO-affiliated organizations, suggesting an intent to conduct future intrusions against this target set." The most frequently hacked organizations in Ukraine are in its government, communications, and energy sectors.[16] That Microsoft has granular data which it has shared about Poland's spillover position sends an important message to NATO. While the attacks, thus far, against Poland have not been egregiously startling, that they occurred at all reinforces a norm that cyberattack is not the same as the kinetic variety. One preliminary hypothesis is that Moscow might in fact believe that cyber actions which cause serious economic, and potentially, physical damage, might not trigger the Article 5 collective defense threshold, or that Russia's cyberattacks at most would trigger a "proportionate response."

We doubt the explanation is effective Russian or Ukrainian battlefield cyber action, which in any event is not making the news. The Fancy Bear/APT28 Russian cyber group, "believed by US intelligence officials to work primarily on behalf of the GRU," has been a significant presence in cyber operations against Ukraine since 2014.[17] Known for its résumé of destructive cyber-attacks, the GRU's cyber forces have attempted to attack Ukrainian infrastructure, but at least one operation against an industrial control system in the country was identified before significant damage occurred.[18] Among combat information systems, Russia has had little visible success in hacking Ukraine's Integrated Air Defense System similar to what Israel achieved with its strike on Syria's nuclear facility in 2007. This does not mean cyberspace-collected intelligence hasn't been effective. Targeting of a Ukrainian precision-guided strike on the Russian barracks at Makiivka on January 1, 2023, likely was enabled by concentrated mobile phone use by the Russian soldiers housed there.[19]

Other academics have produced a considerable volume of writing on the Ukraine war's cyber component. Kenneth Geers draws upon his experience as a cybersecurity researcher in Ukraine in his overview of Russian cyberattacks against Ukraine, both before and during the invasion.[20] Kristen Eichensehr notes the limited role taken of cyber operations in the Ukraine war and considers the ramifications for this on international law.[21] Nadiya Kostyuk and Erike Gartzke present a statistical analysis of 11 years of recent military campaigns and find that "cyber operations are rarely used as either complements to or substitutes for conventional military operations."[22] Joshua Rovner's observations track ours, including the seeming importance of cyberattacks as part of a military campaign and the corresponding absence of Russian effectiveness.[23] Cyberattacks *should* be particularly effective for *sabotage*, damaging or degrading both cyber and physical assets, without the risks normally associated with human saboteurs, who might be captured or killed. From what we see, their primary use in Ukraine is for *espionage* (e.g., exfiltrating secrets/signals intelligence). Lastly, Gavin Wilde examines how NATO and Russian military theorists view the role of cyberattacks as part of larger military campaigns, discussing a number of cyber failures in prior campaigns. He states:

> The issue is less that Western observers might have overestimated Russia's cyber potential in its war on Ukraine, more that they almost certainly underestimate the complexities and frictions which separate intent from execution, intensity from effect. Particularly in the still murky arena of information warfare, the chasm between theory and practice remains wide.[24]

Perhaps the most important takeaway on cyber activity in Ukraine's nearly two-year-old war with Russia is that cyberattacks may only be a small part of the conflict. That said, we can see important developments in adjacent areas, including in computational information or propaganda operations as well as the collection of intelligence. Cyber is neither boon nor bust, but rather a piece of military capability that remains difficult for its users to calibrate and hardly an alternative to all other modes of force. It may hold true that, "cyber operations offer a novel instrument of power below the threshold of war, creating a new strategic space of competition," in areas of non-military or hybrid conflict.[25] In major conflict, cyber operations are part of a larger mix of activity designed to produce military outcomes or alter opinion.

COMMUNICATION BREAKDOWN

We expected Russia to do much to confuse and confound the Ukrainians with cyber action and with strategic and battlefield communications at the top of their target list. We did not anticipate a manifold breakdown in Russian communications among units moving into Ukraine and attempting to coordinate complex operational maneuvers in multiple thrusts across hundreds of kilometers of frontage.[26] We saw ample evidence of Russia not having secure communications at the tactical and operational level. Russian encrypted communications were an abysmal failure.[27] This was clear when a staff officer in the field had to report the death of his commander, Maj. Gen. Vitaly Gerasimov, to their headquarters in Tula, Russia. His request for a secure line was rebuffed, as his commander stated that the encrypted telephones did not work. The message was intercepted and then shared with the world.[28]

Faced with nonsecure and dysfunctional battlefield communications, Russian commanders shifted to what did work—chiefly cellular telephones,[29] often operating on the Ukrainian phone network.[30] This allowed Ukraine access to these calls, some of which they have published, and of course, to geolocate those phones. In at least one instance, the tactic was used to target and kill a Russian general.[31] Conversely, we might have expected Russia to hack the Ukrainian cellular networks, giving them the same advantages—particularly when we have known for years that among other Russian electronic warfare capabilities,[32] Russian unmanned aerial vehicles (UAVs) are capable of acting as deceptive cellular base stations.[33] US cyber assistance may have helped blunt or defeat Russian cyberattacks in this arena,[34] and/or Ukrainian troop phone use may have grown more disciplined; for example, Ukrainian troops are instructed to walk 400 to 500 meters away from their position before using a phone.[35]

Some suggest that Russia has an advantage in keeping the Ukrainian cellular network operational, both for its own communications and to hack Ukrainian targets.[36] Certainly, quiet surveillance over Ukrainian communications could be advantageous to Russia's military. Cellular communications are still an important piece of tactical intelligence, not least for their importance to reconnaissance and attack by drone. Russia's narrower strategy now focusing only on Ukraine's East may make it easier to deploy Russia's electronic warfare systems,[37] and thereby degrade Ukraine's air defense radar and other communications with heavy and adaptive jamming in the radio frequency spectrum. This includes the remote operation of unmanned aerial vehicles (UAVs).

DRONE HELL

In his study of military innovation, Max Boot reminds us that new weapons can remake the conduct of war.[38] Of import in the Ukraine war, perhaps more than any other, is unmanned aircraft. A lesson from the most recent Armenia-Azerbaijan conflict is that the side that masters the employment of drones (a.k.a. unmanned aerial vehicles) may hold a critical advantage.[39] Before fighting broke out, drones were identified as an important equalizer for Ukraine,[40] and this has proven accurate. Two forms of drones, the cheap quadcopter and the heavier medium-endurance UAV, have transformed the information picture that is battlefield situational awareness. Each deserves some attention.

Cheap quadcopters have made an incredible impact in tactical reconnaissance in the region surrounding the forward line of troops. For example, the widely available DJI Phantom 4 Pro offers tremendous observation capability with a 20 megapixel camera producing 4K video recorded or 1080p video live streamed, while operating at a distance of 10 kilometers, with an endurance of 30 minutes.[41] Fully equipped, the Phantom 4 Pro costs about $2,000, or one-fortieth the cost of a Javelin fire-and-forget anti-tank missile. Given the prominent role of artillery in the war, these cheap drones have radically improved battlefield situational awareness, targeting, and damage assessment. We have also seen videos from drones, either locally improvised in Ukraine by hobbyists or produced by the Ukrainian military's Aerorozvidka reconnaissance organization,[42] being used to drop grenades on tanks and other armored targets,[43] all deliverables that also carry propaganda value.

Also involved in strikes against Russian forces and infrastructure targets are Turkish-supplied Bayraktar TB2 UAVs. While the TB2 appears clunky next to US military UAVs, Ukraine has used them to great effect, both for surveillance and to launch missiles. The shift from manned aircraft to unmanned UAVs in reconnaissance and close air support already proved effective in Iraq and Afghanistan, but analysts were concerned about whether they would be as effective in areas with more sophisticated air search radars and electronic warfare. The answer appears to be that effectiveness is situational in nature. In essence, when the opponent has gaps in sensor and air-defense coverage—as Russian forces did during their shambolic early assault on Ukraine in 2022—larger strike and observation drones like the TB2 can operate more aggressively. But once the opponent elevates the quality of electronic warfare operations and brings kinetic air defenses (i.e. surface to air missiles or fighter aircraft) fully into play, the environment becomes far less permissible for a TB2-type UAV.[44] At the lower rungs of the UAV ecosystem (loitering munitions and smaller observation and strike drones), Russian and Ukrainian forces are engaged in a rapid Darwinian contest pitting Russian jammers against Ukrainian observers and attackers.[45]

Ukraine's drone warfare activities evolving substantially. Kyiv's forces have been availing themselves of improvements to range and quantity. Then-Ukrainian Defense Minister Oleksii Reznikov told Reuters in March 2023 that Ukraine is working with over 80 indigenous drone makers.[46] As it taps this diverse technical ecosystem, defense officials appear to show particular interest in long-ranged strike drones, including tests announced in December 2022 that allegedly involved a 1,000-km range strike drone. If production can be scaled up and especially, if Ukrainian manufacturers can obtain sufficient NATO support for a high-capability "drone parts bin," Kyiv could deploy a symmetrical answer to the Shahed drones Russia has been launching at targets across Ukraine for months.[47] Multiple drone attacks on Moscow during the summer of 2023 foreshadow what could evolve into a broader, higher intensity campaign more akin to the Houthi drone war against Saudi Arabia and the UAE in recent years.[48]

Coming months may also see qualitative increases in Ukrainian drone capability, potentially including the first combat use of networked drone swarms. Of particular note, the 24 February 2023 US military aid package to Ukraine included Anduril's Altius-600, launchable from many platforms, with a range exceeding 250 miles, and is capable of operating in a networked swarm.[49] Observers should also expect additional strikes on Russian energy and critical infrastructure in response to Moscow's targeting of Ukraine's power grid.[50] As the Ukrainian Air Force acquires F-16s, it may also (as Israel has) seek persistent anti-radiation loitering munitions for air defense suppression and destruction missions. It is also likely that more intense and widespread drone-on-drone aerial combat will take place in Ukraine and that the country's east and south will effectively be a global laboratory for such activity.[51] The bottom line is that as the war heads into 2024, the drone space will combine creativity and innovation, while calling for greater industrial mass on the basis that while drones are game changing, they exert their most profound effects when deployed in large quantities.

INTELLIGENCE AND THE INFORMATION WAR

Russia's supposedly pervasive penetration of Ukrainian political and economic structures failed at the most basic level to yield accurate intelligence about Kyiv's willingness to fight. Had the Russians received or accepted better information and been able to premise their assumptions on something closer to reality, they might have structured an entirely different attack plan and been more successful in meeting less ambitious goals than taking down Kyiv and much of the country in a matter of days. Putin reminds us that intelligence is fed to political leaders who often ignore or dismiss it due to their own cognitive blinders or ambitions.[52]

In the West, intelligence regarding the war has been abundant, accurate, and publicly disseminated. For example, the U.K.'s Ministry of Defense has been publishing daily summaries on its Facebook page. In the days prior to Russia entering Ukraine, American and British public statements accurately predicted Russian actions before they happened.[53] Demonstrably, Russia was unable to protect the confidentiality of its planning and deliberation process, with US intelligence operations having thoroughly penetrated Russia's political leadership, spying apparatus, and military.[54] Russian denials at the time proved false, damaging Russian credibility as to other statements they have made since, thereby bolstering the legitimacy of NATO information releases. While the US and its allies predictably have yet to disclose their sources or methods, the scope and breadth of their disclosures were certainly a surprise. "It doesn't have to be solid intelligence," one US official said. "It's more important to get out ahead of [the Russians], Putin specifically, before they do something."[55] This rapid dissemination represents a paradigm change in how intelligence is processed, leading to a variety of benefits—including reports that Russia delayed its own invasion timetable, which allowed NATO allies more time to coordinate response.

Relatively little has been written about cyber intelligence operations against Russia by Ukraine and its allies, although there have been suggestions that NATO forces have contributed targeting data for high-value targets such as munitions depots and command centers. Employment of HIMARS, an artillery rocket launcher, and its long-range (~90 km) guided rocket GLMRS,[56] have yielded spectacular results in destroying ammunition depots and command targets.[57] Such targeting information undoubtedly was cyber-enhanced, for example, by hacking and tracking cellular telephones or even by hacking into Russian military command networks; or more traditional signals intelligence operations (e.g., triangulating the locations of radars and radios); or by satellite reconnaissance; and/or from observers and drones on the frontlines.

There was a reported leak of US military classified information, where photographs of printed documents appeared on various Internet chat rooms and social media.[58] News reports appear to confirm two important facts. First, they confirm that the US and its allies have extensively compromised Russian government sources. They also reveal a US security vulnerability, or perhaps a compromised insider, leaking sensitive US intelligence. Some of the leaked documents reportedly appear to have been modified to make it appear that Russian casualties were lower and Ukrainian casualties were higher, suggesting that the leak at least in part was calculated propaganda, a subject covered in the next section.

It is also entirely possible that cyber operations have degraded Russian military capabilities. In another context, for example, Israel allegedly hacked a Syrian radar system[59] prior to bombing the Al Kubar nuclear facility in 2007.[60] We note that the same Russian S-300 radars used by Syria in 2007 are fielded by Russia in Ukraine today, so it is conceivable that some Ukrainian military operations have tried something similar. The Russians may also be attempting to glean cyber intelligence. They have done so before. One curious episode, unearthed in 2016, concerned a Ukrainian homegrown cell phone app for artillery targeting, which Russia's military was able to compromise, giving it real-time geolocations of Ukrainian artillery units.[61] This is exactly the kind of cyber intelligence activity that we would have expected to happen in the current war. If it is happening, it is not making the news.

What we do know about is the relevance of open-source intelligence (OSINT). At least at the beginning of the war, any Ukrainian with a camera who filmed an attack on a Russian armored vehicle seemed to post it on the internet. Those images, in aggregate, plus videos posted by the Ukrainian and Russian militaries, often from UAVs, provide a surprisingly comprehensive view of the war. They are also increasingly studied by large, distributed amateur and scholarly communities. King's College Ph.D. student and former US Marine officer Rob Lee,[62] among others, strung together a collage of online media to create a compelling analytic narrative of the war. Non-governmental groups like Bellingcat have collected data and developed guides and tools for others to use (e.g., for Telegram and TikTok).[63] No doubt machine learning techniques and increasingly sophisticated geo-indexed imagery sources can paint vivid battlefield pictures.[64] There is even an OSINT component to understanding the cyber war, evinced by raw reporting from security researchers and government/civil society and aggregated in a CSIS report.[65]

PROPAGANDA, MISINFORMATION, AND DISINFORMATION

Many assumed that Russia was powerfully strong in enhancing and exploiting influence operations using cyberspace.[66] Russia's combination of computer hacking and targeted propaganda in both the U.K. Brexit referendum and US national elections in 2016 revealed highly sophisticated skill in undermining NATO democratic institutions. We have come to expect online active measures that confound NATO democracies,[67] yet Ukraine has dominated the information war for public support. In information operations, Ukraine has been able to transform leaked, unsecure Russian communications into a video of anti-armor ambushes[68] and a narrative of triumph over a hapless opponent. Ukraine has waged a media war that effectively portrays itself as a victim it is, and that effectively reveals the terrible price Russia has paid thus far for its invasion. The retreat of Russian forces from the outskirts of Kyiv scored additional propaganda points.

Ukraine's need from the West for more modern weaponry has been an incessant and ongoing information campaign by the country that has been highly successful.[69] From the first day of combat, Ukraine's leaders have made the case repeatedly for modern armaments able to give it a qualitative edge on the battlefield. Videos uploaded to Telegram, Twitter, YouTube, and other social media platforms weaved a narrative of plucky Ukrainian light infantry repeatedly visiting chaos and calamity on Russian mechanized units. This success begat requests for more arms, accompanied by videos of precision-guided destruction once fielded. Kyiv's public efforts to influence Western countries to fill its dire need for replacement tanks and armored vehicles peaked with President Zelenskyy's late 2022 visit to the US, which was presaged with a video in which Bob Seeger's "Like a rock" riff once found in Chevrolet truck commercials became the soundtrack for a mash-up of American-built heavy armor.[70]

Russian propaganda, internally targeted, has bolstered support at home, although Russia has also aggressively cracked down on and jailed its internal activists.[71] How successful they are ultimately remains to be seen, but Russia has invested heavily in efforts to hobble its domestic news media and limit access to the broader internet.[72] For the Ukrainian territories occupied by Russian forces, Russia has rerouted internet traffic through its own ISPs censorship regime.[73]

Outside of its own borders, Russia has been ineffective at countering Ukraine's narrative. From the outset, Russia repeatedly has claimed that Ukraine is filled with "Nazis,"[74] and they continue to traffic this palpably false claim, both internally and externally. Russian propaganda efforts regarding Ukraine appear borne of an unreality hard for almost anyone to accept as true, but those efforts continue nonetheless.[75] To add to this incompetence, Russian propaganda has led to successful, deadly targeting of Russian forces. Ukraine undoubtedly was fully aware of Russian news reports of maritime logistical operations in the port of Berdyansk when it prepared its standoff missile attacks against Black Sea Fleet amphibious ships.[76] And despite being under Russian control, video from Berdyansk of a sinking Russian ship and the strikes against two others leaked online.[77] Russian-controlled footage also emerged online of the severely damaged Black Sea Fleet flagship, *Moskva*, before it sank.

WHAT'S COMING NEXT?

Wisdom is shown again and again with the aphorism, "it's difficult to make predictions, especially about the future." We will not try to predict the future of kinetic warfare in Ukraine, which depends on a variety of unknowns, including what weapons Ukraine is able to adopt and how effective it will be at blunting Russia's attacks. Likewise, we cannot predict whether NATO sanctions against Russia and its oligarchs will yield sufficient domestic political pressure for Russia to either convince Putin to withdraw or to convince others to overthrow him. What we can predict is that both sides will increasingly look to cyber tactics to support kinetic warfare as well as support propaganda and information operations.

For kinetic warfare, we are already seeing a variety of NATO armaments being delivered to Ukraine, many of which include precise GPS targeting capabilities. This suggests Russia might counter with GPS jamming/spoofing. It also suggests that broader packages of the latest electronic warfare equipment might be necessary for Ukraine to continue to fight.[78] Clark, an expert on Russia's portfolio of electronic warfare systems, including jammers, attack tools, counterattack tools, and surveillance equipment, explains how ineffective they have been for most of the war, becoming relevant only once the battle lines became relatively static in Eastern Ukraine.[79]

Propaganda operations undoubtedly will grow more sophisticated on both sides. Today's propaganda largely entails the release of news and videos to broad audiences. Even though TikTok's short videos might be a novel delivery mechanism, the idea of using videos for propaganda purposes is nothing new. What we expect to see going forward is *microtargeted propaganda*. Much as Russian operatives used Facebook's advertisement targeting features to identify and manipulate US voters in the lead-up to the 2016 election,[80] we can and should expect similar microtargeting to on the Ukraine war, to include Russia attempting to manipulate US or other NATO elections and the election of less Ukraine-sympathetic leadership. It is also likely that Russian propaganda and cyber-hacking efforts will target other countries that have emerged as key Ukraine allies. For example, Albania, which has offered public support to Ukraine and has taken in a huge number of Ukrainian refugees, experienced a cyberattack forcing it to take down a number of government services.[81] This activity is now playing out on the information systems of multiple NATO countries, principally located near Russia and Ukraine.

Closer to the battlefield, attempts to manipulate soldier morale are as old as warfare itself. We know Russia has sent messages to Ukrainian phones (both soldiers and their families) and volunteers are sending pro-Ukrainian messages to random Russian phone numbers and posting them to Russian restaurant review sites.[82] Going forward, imagine individual soldiers receiving tailored text messages should come as no surprise: "Here's a photo of you at this location today. We'll kill you there tomorrow if you don't lay down your arms and leave." On top of that, Ukraine could leverage its war crimes accountability and documentation efforts[83] with tailored messages, e.g., "We know you were ordered to do X, which would make you personally liable as a war criminal. Don't do it." Such messages could even be created as group texts with the soldiers' families, perhaps inferred from text message interception, in an attempt to leverage family ties to break soldier morale. Moreover, as word spreads at home, this would dissuade other civilians from enlisting for voluntary military service, and/or further encourage their exodus from Russia.[84] It is also completely reasonable to imagine Ukraine sending informative text messages to recently arriving Russian soldiers, e.g., "Welcome to Luhansk. Here's a link to your instruction on the Geneva Convention and war crimes."

One curious aspect of cyber effects in warfare is that they arguably raise less risk of escalation, with cyberattacks on nuclear command and control being a notable exception.[85] NATO's caution against Russian escalation has clearly limited the weapon flow to Ukraine. For example, the US has long supplied Ukraine with HIMARS artillery rocket systems, but delayed supplying the longer-range ATACMS. This contrasts with cyber operations, which the US can conduct itself without providing any technology directly to Ukraine, much less putting any American operator in harm's way.[86] While the details of US cyber operational support for Ukraine are not publicly disclosed, it is widely reported that US and other allied cyber operations are working closely to support Ukraine, and this very likely will continue.[87]

CONCLUSION

This article considers many ways in which revolutionary technologies have impacted the Ukraine war.[88] We expected Russians to successfully mount sophisticated cyberattacks, both in terms of espionage and sabotage, against the Ukrainians, but this did not happen in any fashion that would have been decisive to the war. If anything, Ukraine has outperformed Russia, both in its cyber defense and its counterattacks (often with key aid from its NATO supporters).

We could easily conclude that Russia's cyber corps failed, or that cyber-effects are a minor component of Russia's overall military strategy. Perhaps a more nuanced view might be to conclude that this is but one of myriad aspects of Russia's military that so far has failed, to include its command and control, logistics, air forces, and navy. Pointing to anything going particularly well for Russia in this war is a challenge, which implicates failure at the highest echelons of Russia's military and civilian leadership.

Perhaps the question we ask, instead is why Russia has done so poorly with its cyber and information forces and why Ukraine has been so successful. It appears that a vigilant and prepared defender can stand up to the information and cyber punishment that may be dealt out by the Kremlin. Important lessons can be derived both from the ongoing war and for future contingencies.

NOTES

1. While Russia calls it a “special military operation,” we refer to it in this essay as the “Ukraine War.” We also use “NATO” and “NATO allies” to include countries assisting Ukraine, including those not NATO members.
2. Harris, Shane, and Dan Lamothe. 2022. “U.S. rules for sharing intelligence with Ukraine.” *The Washington Post*, May 11, 2022, https://www.washingtonpost.com/national-security/2022/05/11/ukraine-us-intelligence-sharing-war/.
3. Milmo, Dan. 2022. “China accused of cyber-attacks on Ukraine before Russian invasion.” *The Guardian*, April 1, 2022. https://www.theguardian.com/technology/2022/apr/01/china-accused-of-launching-cyber-attacks-on-ukraine-before-russian-invasion.
4. O’Neill, Patrick. 2022. Russia hacked an American satellite company one hour before the Ukraine invasion. MIT Technology Review, May 10, 2022.
5. Kan, Michael. 2022. “Pentagon Impressed by Starlink’s Fast Signal-Jamming Workaround in Ukraine.” PCMag, April 21, 2022. https://www.pcmag.com/news/pentagon-impressed-by-starlinks-fast-signal-jamming-workaround-in-ukraine.
6. Harris, Shane, Karen DeYoung, Isabelle Khurshudyan, Ashley Parker, and Liz Sly. 2022. “As Russia prepared to invade Ukraine, U.S. struggled to convince Zelensky, allies of threat.” *The Washington Post*, August 16, 2022. https://www.washingtonpost.com/national-security/interactive/2022/ukraine-road-to-war/.
7. Assante, Michael. 2016. “SANS Industrial Control Systems Security Blog | Confirmation of a Coordinated Attack on the Ukrainian Power Grid.” SANS Institute, https://www.sans.org/blog/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid/.
8. Greenberg, Andy. 2018. “The Untold Story of NotPetya, the Most Devastating Cyberattack in History.” *WIRED*, August 22, 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.
9. Hofmann, Frank. 2022. “Russia's hybrid war against Ukraine | Europe | News and current affairs from around the continent.” *DW*, February 18, 2022. https://www.dw.com/en/russias-hybrid-war-against-ukraine/a-60829873.
10. Harding, Emily. 2022. “The Hidden War in Ukraine | Center for Strategic and International Studies.” Center for Strategic and International Studies, https://www.csis.org/analysis/hidden-war-ukraine.
11. Smith, Brad. 2022. “Defending Ukraine: Early Lessons from the Cyber War - Microsoft On the Issues.” The Official Microsoft Blog, https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/.
12. Smalley, Suzanne. 2022. “Cybersecurity experts question Microsoft’s Ukraine report.” *CyberScoop*, July 1, 2022, https://www.cyberscoop.com/cybersecurity-experts-question-microsofts-ukraine-report/.
13. “Ukraine Network IOCs.” 2022. PasteBin, https://pastebin.com/PCK97yjc.
14. Google. 2023. *Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape*.
15. Willett, Marcus. “The Cyber Dimension of the Russia–Ukraine War.” *In Survival: October-November 2022*, pp. 7-26. Routledge, 2022.
16. Microsoft. 2023. A year of Russian hybrid warfare in Ukraine, March 15, 2023.
17. Volz, Dustin. 2016. “Russian hackers tracked Ukrainian artillery units using Android implant: report.” Reuters, December 21, 2016, https://www.reuters.com/article/us-cyber-ukraine/russian-hackers-tracked-ukrainian-artillery-units-using-android-implant-report-idUSKBN14B0CU.
18. Lehto, M. "Cyber Warfare and War in Ukraine.” *Journal of Information Warfare* 22, no. 1 (2023).
19. Beale, Jonathan. 2023. “Makiivka attack: Could mobile phones have revealed Russian location?” BBC, https://www.bbc.com/news/world-europe-64164921.
20. Geers, Kenneth. 2022. “Computer Hacks in the Russia-Ukraine War.” DEFCON 30, https://media.defcon.org/DEF%20CON%2030/DEF%20CON%2030%20presentations/Kenneth%20Geers%20-%20Computer%20Hacks%20in%20the%20Russia-Ukraine%20War%20-%20paper.pdf.
21. Eichensehr, Kristen. 2022. “Ukraine, Cyberattacks, and the Lessons for International Law.” *AJIL Unbound* 116:145-149, https://doi.org/10.1017/aju.2022.20.
22. Kostyuk, Nadiya, and Erik Gartzke. 2022. “Why Cyber Dogs Have Yet to Bark Loudly in Russia's Invasion of Ukraine.” *Texas National Security Review* 5, no. 3 (Summer): 113-126, http://dx.doi.org/10.26153/tsw/42073.
23. Rovner, Joshua. 2022. “Sabotage and War in Cyberspace.” *War on the Rocks*, https://warontherocks.com/2022/07/sabotage-and-war-in-cyberspace/.
24. Wilde, Gavin. 2022. “Assess Russia’s Cyber Performance Without Repeating Its Past Mistakes.” *War on the Rocks*, https://warontherocks.com/2022/07/assess-russias-cyber-performance-without-repeating-its-past-mistakes/.

NOTES

25. Maschmeyer, Lennart. “Subversion, cyber operations, and reverse structural power in world politics.” *European Journal of International Relations* 29, no. 1 (2023): 79-103.
26. Cranny-Evans, Sam, and Thomas Withington. 2022. “Russian Comms in Ukraine: A World of Hertz.” RUSI, https://rusi.org/explore-our-research/publications/commentary/russian-comms-ukraine-world-hertz.
27. Myre, Greg. 2022. “How does Ukraine keep intercepting Russian military communications?” NPR, https://www.npr.org/2022/04/26/1094656395/how-does-ukraine-keep-intercepting-russian-military-communications.
28. Borger, Julian. 2022. “Vitaly Gerasimov: second Russian general killed, Ukraine defence ministry claims.” *The Guardian*, March 9, 2022, https://www.theguardian.com/world/2022/mar/08/vitaly-gerasimov-second-russian-general-killed-ukraine-defence-ministry-claims.
29. Schogol, Jeff. 2022. “US military learning from Russian troops using cell phones in Ukraine.” *Task & Purpose*, May 13, 2022, https://taskandpurpose.com/news/russia-ukraine-cell-phones-track-combat/.
30. Horton, Alex, and Shane Harris. 2022. “Russian troops' tendency to talk on unsecured lines is proving costly.” *The Washington Post*, March 27, 2022, https://www.washingtonpost.com/national-security/2022/03/27/russian-military-unsecured-communications/.
31. Schmitt, Eric. 2022. “As Russian Troop Deaths Climb, Morale Becomes an Issue, Officials Say.” *The New York Times*, March 16, 2022, https://www.nytimes.com/2022/03/16/us/politics/russia-troop-deaths.html.
32. Kadam, Tanmay. 2022. “Russia's Electronic Warfare Capability 'Exposed' In Ukraine War; Is Putin's Techno-Savvy Army Losing The EW Battle?” *EurAsian Times*, April 18, 2022, https://eurasiantimes.com/russias-electronic-warfare-capability-exposed-in-ukraine-war/.
33. Peck, Michael. 2017. “The Crazy Way Russia Could Hijack Your iPhone.” *The National Interest*, April 2, 2017, https://nationalinterest.org/blog/the-buzz/the-crazy-way-russia-could-hijack-your-iphone-19976.
34. Srivastava, Mehul, Madhumita Murgia, and Hannah Murphy. 2022. “The secret US mission to bolster Ukraine's cyber defences ahead of Russia's invasion.” *Financial Times*, March 8, 2022, https://www.ft.com/content/1fb2f592-4806-42fd-a6d5-735578651471.
35. Devine, Kieran. 2022. “Ukraine war: Mobile networks being weaponised to target troops on both sides of conflict.” Sky News, April 1, 2022, https://news.sky.com/story/ukraine-war-mobile-networks-being-weaponised-to-target-troops-on-both-sides-of-conflict-12577595.
36. Sabin, Sam, and Laurens Cerulus. 2022. “3 reasons Moscow isn't taking down Ukraine's cell networks.” Politico, March 7, 2022, https://www.politico.com/news/2022/03/07/ukraine-phones-internet-still-work-00014487.
37. Clark, Bryan. 2022. “The Fall and Rise of Russian Electronic Warfare.” *IEEE Spectrum*, July 30, 2022. https://spectrum.ieee.org/the-fall-and-rise-of-russian-electronic-warfare.
38. Boot, M., 2006. War made new: technology, warfare, and the course of history, 1500 to today, Penguin.
39. Dixon, Robyn. 2020. “Azerbaijan's drones owned the battlefield in Nagorno-Karabakh — and showed future of warfare.” *The Washington Post*, November 11, 2020, https://www.washingtonpost.com/world%2Feurope%2Fnagorno-karabkah-drones-azerbaijan-aremenia%2F2020%2F11%2F11%2F441bcbd2-193d-11eb-8bda-814ca56e138b_story.html.
40. Bronk, Chris, and Gabriel Collins. 2021. “Bear, Meet Porcupine: Unconventional Deterrence for Ukraine.” Defense One, https://www.defenseone.com/ideas/2021/12/bear-meet-porcupine-unconventional-deterrence-ukraine/360195/.
41. “Phantom 4 Pro V2.0.” n.d. DJI. Accessed August 23, 2022, https://www.dji.com/phantom-4-pro-v2.
42. “Aerorozvidka.” n.d. Wikipedia. Accessed August 23, 2022. https://en.wikipedia.org/wiki/Aerorozvidka.
43. Hambling, David. 2022. “Ukrainian Drone Drops Bomb Through Open Hatch To Score First Kill On Russia’s Oldest Tank.” *Forbes,* July 7, 2022, https://www.forbes.com/sites/davidhambling/2022/07/07/ukrainan-drop-drone-bomb-through-open-hatch-to-score-first-kill-on-russias-oldest-tank/?sh=63cf770f36c6.
44. See, for instance: Agnes Helou, “With Turkish drones in the headlines, what happened to Ukraine’s Bayraktar TB2s?,” Breaking Defense, 6 October 2023, https://breakingdefense.com/2023/10/with-turkish-drones-in-the-headlines-what-happened-to-ukraines-bayraktar-tb2s/
45. Hambling, David. 2023. “How Have Ukrainian Drones Beaten Russian Jammers — And Will It Last?” Forbes, 9 August 2023, https://www.forbes.com/sites/davidhambling/2023/08/09/how-did-ukraine-beat-russias-drone-jammers/?sh=-1c0afac97caa
46. Hunder, Max. 2023. “Inside Ukraine’s scramble for ‘game-changer’ drone fleet.” *Reuters*. March 24, 2023, https://www.reuters.com/world/europe/inside-ukraines-scramble-game-changer-drone-fleet-2023-03-24/

NOTES

47. Collins, Liam. 2018. “Russia Gives Lessons in Electronic Warfare | AUSA.” Association of the United States Army, July 26, 2018. https://www.ausa.org/articles/russia-gives-lessons-electronic-warfare.

48. “More drones coming, Ukraine tells Russia after skyscraper hit,” BBC, 1 August 2023, https://www.bbc.co.uk/news/live/world-66367658. See also: Collins, Gabriel. 2023. “Ukraine Needs Long-Range Firepower for Victory.” Foreign Policy. January 4, 2023. https://foreignpolicy.com/2023/01/04/ukraine-long-range-firepower-victory/ and Bronk, Christopher and Gabriel Collins. “Ukraine Needs a Whole Lot of Deadly Drones.” Foreign Policy. April 13, 2022. https://foreignpolicy.com/2022/04/13/ukraine-drone-warfare-armaments-russia/

49. Newdick, Thomas. 2023. “Putin Admits Moscow’s Air Defenses “Need Work” After Multi-Drone Attack.” May 30, 2023. The Drive, https://www.thedrive.com/the-war-zone/putin-admits-moscows-air-defenses-need-work-after-multi-drone-attack.

50. “SBU drones hit power substation feeding military facilities in Russia’s Belgorod region.” 2023. Ukrinform. October 15, 2023, https://www.ukrinform.net/rubric-ato/3774242-sbu-drones-hit-power-substation-feeding-military-facilities-in-russias-belgorod-region.html

51. “How drones dogfight above Ukraine.” 2023. The Economist. February 7, 2023. https://www.economist.com/the-economist-explains/2023/02/07/how-drones-dogfight-above-ukraine

52. Fingar, Thomas. 2011. *Reducing uncertainty: Intelligence analysis and national security*, Stanford University Press.

53. Sabbagh, Dan. 2022. “Drone footage shows Ukrainian ambush on Russian tanks.” *The Guardian*, March 11, 2022, https://www.theguardian.com/world/2022/mar/10/drone-footage-russia-tanks-ambushed-ukraine-forces-kyiv-war.

54. Harris, Shane, Karen DeYoung, Isabelle Khurshudyan, Ashley Parker, and Liz Sly. 2022. “As Russia prepared to invade Ukraine, U.S. struggled to convince Zelensky, allies of threat.” *The Washington Post*, August 16, 2022, https://www.washingtonpost.com/national-security/interactive/2022/ukraine-road-to-war/.

55. Dilanian, Ken, Courtney Kube, Carol Lee, and Dan De Luce. 2022. “Bold, effective and risky: The new strategy the U.S. is using in the info war against Russia.” *NBC News*, https://www.nbcnews.com/politics/national-security/us-using-declassified-intel-fight-info-war-russia-even-intel-isnt-rock-rcna23014.

56. “M142 HIMARS.” n.d. Wikipedia. Accessed August 23, 2022, https://en.wikipedia.org/wiki/M142_HIMARS.

57. Hunder, Max, Tom Balmforth, and Timothy Heritage. 2022. “Ukrainian military strikes with Western arms disrupt Russian supply lines - general.” Reuters, July 14, 2022, https://www.reuters.com/world/europe/ukrainian-military-strikes-with-western-arms-disrupt-russian-supply-lines-2022-07-14/.

58. Barnes, Julian E., Helene Cooper, Thomas Gibbons-Neff, Michael Schwirtz, and Eric Schmitt, “Leaked Documents Reveal Depth of U.S. Spy Efforts and Russia’s Military Struggles,” *The New York Times*, April 8, 2023, https://www.nytimes.com/2023/04/08/us/politics/leaked-documents-russia-ukraine-war.html.

59. Gasparre, Richard. 2008. “The Israeli 'E-tack' on Syria – Part II.” *Airforce Technology*, https://www.airforce-technology.com/analysis/feature1669/.

60. Farrell, Stephen. 2018. “Israel admits bombing suspected Syrian nuclear reactor in 2007, warns Iran.” Reuters, March 20, 2018, https://www.reuters.com/article/us-israel-syria-nuclear/israel-admits-bombing-suspected-syrian-nuclear-reactor-in-2007-warns-iran-idUSKBN1GX09K.

61. Martin, David. 2016. “Russian hacking proves lethal after Ukrainian military app hijacked.” CBS News, https://www.cbsnews.com/news/russian-hacking-proves-lethal-after-ukrainian-military-app-compromised/.

62. Lee, Rob. 2022. “Rob Lee (@RALee85).” Twitter, https://twitter.com/RALee85.

63. 2022. Bellingcat - the home of online investigations, https://www.bellingcat.com.

64. Tearline. 2022. “Ukraine.” Tearline.mil, https://www.tearline.mil/category/ukraine/.

65. Harding, Emily. 2022. “The Hidden War in Ukraine | Center for Strategic and International Studies,” https://www.csis.org/analysis/hidden-war-ukraine.

66. Cordey, Sean. 2019. “Cyber Influence Operations: An Overview and Comparative Analysis,” ETHZ Research Collection, https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/382358/1/Cyber-Reports-2019-10-CyberInfluence.pdf.

67. Rid, Thomas. 2020. *Active Measures: The Secret History of Disinformation and Political Warfare.* N.p.: Farrar, Straus and Giroux.

68. Sabbagh, Dan. 2022. “Drone footage shows Ukrainian ambush on Russian tanks.” *The Guardian*, March 11, 2022, https://www.theguardian.com/world/2022/mar/10/drone-footage-russia-tanks-ambushed-ukraine-forces-kyiv-war.

69. Dyczok, Marta, and Yerin Chung. “Zelens'kyi uses his communication skills as a weapon of war.” *Canadian Slavonic Papers* 64, no. 2-3 (2022): 146-161.

NOTES

70. Even two of the authors added their voices to the chorus on sending Ukraine modern, Western tanks. Collins, Gabriel and Chris Bronk. 2023. "The M1 Abrams is the Right Tank for the Job in Ukraine." *Foreign Policy*, January 24, 2023.
71. Dixon, Robyn. 2022. "In Putin's Russia, antiwar protesters face prison and abuse." *The Washington Post*, June 26, 2022, https://www.washingtonpost.com/world/2022/06/26/russia-protests-dissent-activists-skochilenko/.
72. McMahon, Robert, and Emily Lieberman. 2022. "Russia Is Censoring News on the War in Ukraine. Foreign Media Are Trying to Get Around That." Council on Foreign Relations, https://www.cfr.org/in-brief/russia-censoring-news-war-ukraine-foreign-media-are-trying-get-around.
73. Satariano, Adam, and Lindsey Balbierz. 2022. "How Russia Took Over Ukraine's Internet in Occupied Territories." *The New York Times*, August 9, 2022, https://www.nytimes.com/interactive/2022/08/09/technology/ukraine-internet-russia-censorship.html.
74. Srulevitch, Andrew. 2022. "Why is Putin Calling the Ukrainian Government a Bunch of Nazis?" ADL. https://www.adl.org/blog/why-is-putin-calling-the-ukrainian-government-a-bunch-of-nazis. Also see: Cloud, David S., James Marson, Evan Gershkovich, and Laurence Norman. 2022. "Russia Ramps Up Accusations of Neo-Nazism in Ukraine." *The Wall Street Journal*, May 3, 2022, https://www.wsj.com/articles/russia-reiterates-accusations-of-neo-nazism-in-ukraine-11651579622.
75. Rossoliński-Liebe, Grzegorz, and Bastiaan Willems. "Putin's Abuse of History: Ukrainian 'Nazis','Genocide', and a Fake Threat Scenario." *The Journal of Slavic Military Studies* 35, no. 1 (2022): 1-10.
76. BBC. 2022. "Russian warship destroyed in occupied port of Berdyansk, says Ukraine," March 24, 2022, https://www.bbc.com/news/world-europe-60859337.
77. Sutton, H. I. 2022. "Satellite Images Confirm Russian Navy Landing Ship Was Sunk at Berdyansk - *USNI News*." USNI News, March 25, 2022, https://news.usni.org/2022/03/25/satellite-images-confirm-russian-navy-landing-ship-was-sunk-at-berdyansk.
78. LaPorta, James. 2018. "Lockheed's 'Dragon Shield' for Finland achieves operational capability." UPI, February 12, 2018, https://www.upi.com/Defense-News/2018/02/12/Lockheeds-Dragon-Shield-for-Finland-achieves-operational-capability/2281518445772/.
79. Clark, Bryan. 2022. "The Fall and Rise of Russian Electronic Warfare." *IEEE Spectrum,* July 30, 2022, https://spectrum.ieee.org/the-fall-and-rise-of-russian-electronic-warfare.
80. Mayer, Jane. 2018. "How Russia Helped Swing the Election for Trump." *The New Yorker*, September 24, 2018, https://www.newyorker.com/magazine/2018/10/01/how-russia-helped-to-swing-the-election-for-trump.
81. *Euronews Albania.* 2022. "'Sulm kibernetik nga jashtë Shqipërisë', AKSHI bllokon shërbimet online." July 17, 2022, https://euronews.al/vendi/aktualitet/2022/07/17/sulm-kibernetik-nga-jashte-shqiperise-akshi-bllokon-sherbimet-online/.
82. Cecil, Nicholas. 2022. "Putin's forces sending threats to phones of Ukraine's soldiers, say defence experts." *Evening Standard*, June 10, 2022. https://www.standard.co.uk/news/world/vladimir-putin-war-ukraine-russia-psychological-warfare-institute-for-the-study-of-war-b1004992.html. Also: Collins, Liam. 2018, "Russia Gives Lessons in Electronic Warfare | AUSA." Association of the United States Army, July 26, 2018. https://www.ausa.org/articles/russia-gives-lessons-electronic-warfare. Gronholt, Jacob. 2022. "Keyboard army using restaurant reviews to take on Russian state media." Reuters, March 3, 2022. https://www.reuters.com/world/europe/keyboard-army-using-restaurant-reviews-take-russian-state-media-2022-03-02/. Zitser, Joshua. 2022, "Ukraine: Meet the Volunteers Messaging Random Russians to Tell of Putin's War," *Business Insider*, March 19, 2022, https://www.businessinsider.com/ukraine-meet-the-volunteers-messaging-random-russians-tell-putins-war-2022-3.
83. *The New York Times.* 2022. "Documenting Atrocities in the War in Ukraine." May 22, 2022, https://www.nytimes.com/interactive/2022/05/22/world/europe/ukraine-war-crimes.html.
84. Ebel, Francesca and Mary Ilyushina, "Russians abaondon wartime Russia in historic exodus", *The Washington Post*, February 13, 2023, https://www.washingtonpost.com/world/2023/02/13/russia-diaspora-war-ukraine/
85. Acton, James M. 2020. "Cyber Warfare & Inadvertent Escalation." *Daedalus* 149, no. 2 (Spring): 133-149, https://doi.org/10.1162/daed_a_01794.
86. Libicki, Martin C. 2012. "Crisis and Escalation in Cyberspace | RAND." RAND Corporation, https://www.rand.org/pubs/monographs/MG1215.html.
87. Lin, Herbert. "Russian Cyber Operations in the Invasion of Ukraine." *The Cyber Defense Review* 7, no. 4 (2022): 31-46.
88. Robinson, Paul. "The Russia-Ukraine Conflict and the (Un) Changing Character of War." *Journal of Military and Strategic Studies* 22, no. 2 (2022).