HDIAC Homeland Defense & Security Information Analysis Center

HDIAC TECHNICAL INQUIRY (TI) RESPONSE REPORT

Technological Lessons Learned From the Conflict Between Russia and Ukraine

Report Number:
HDIAC-BCO-2023-336
Completed February 2023

HDIAC is a Department of Defense
Information Analysis Center

MAIN OFFICE
4695 Millennium Drive
Belcamp, MD 21017-1505
Office: 443-360-4600

REPORT PREPARED BY:
John Clements
Office: HDIAC

Information contained in this report does not constitute endorsement by the U.S. Department of Defense of any nonfederal entity or technology sponsored by a nonfederal entity.

HDIAC is sponsored by the Defense Technical Information Center, with policy oversight provided by the Office of the Under Secretary of Defense for Research and Engineering. HDIAC is operated by the SURVICE Engineering Company.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*

2. REPORT TYPE
Technical Research Report

3. DATES COVERED *(From – To)*

4. TITLE AND SUBTITLE

Technological Lessons Learned From the Conflict Between Russia and Ukraine

5a. CONTRACT NUMBER
FA8075-21-D-0001

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

John Clements

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Homeland Defense & Security Information Analysis
Center (HDIAC)
SURVICE Engineering Company
4695 Millennium Drive
Belcamp, MD 21017-1505

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Defense Technical Information Center (DTIC)
8725 John J. Kingman Road
Fort Belvoir, VA 22060-6218

10. SPONSOR/MONITOR'S ACRONYM(S)
DTIC

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

DISTRIBUTION A. Approved for public release: distribution unlimited.

13. SUPPLEMENTARY NOTES
air platform: unmanned aircraft system (UAS); autonomous systems
autonomy: human/autonomous system interaction and collaboration; autonomous systems
human systems: social, cultural, and behavioral understanding; cultural studies

14. ABSTRACT

The Homeland Defense and Security Information Analysis Center (HDIAC) was asked to provide lessons learned in the ongoing conflict between Ukraine and Russia. These lessons should apply to both the strategic and tactical levels of combat. The inquirer requested that the research focus on studies from organizations like Federally Funded Research and Development Centers. HDIAC identified lessons in five overarching areas—tactics, unmanned aerial systems/drones, cyber and information warfare, military materiel, and space.

15. SUBJECT TERMS
ground combat, tanks, unmanned aerial system, UAS, drone, information warfare

16. SECURITY CLASSIFICATION OF: U			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** Ted Welsh, HDIAC Director
a. REPORT U	**b. ABSTRACT** U	**c. THIS PAGE** U	UU	17	**19b. TELEPHONE NUMBER** *(include area code)* 443-360-4600

ABOUT DTIC AND HDIAC

The Defense Technical Information Center (DTIC) preserves, curates, and shares knowledge from the U.S. Department of Defense’s (DoD's) annual multibillion dollar investment in science and technology, multiplying the value and accelerating capability to the Warfighter. DTIC amplifies this investment by collecting information and enhancing the digital search, analysis, and collaboration tools that make information widely available to decision makers, researchers, engineers, and scientists across the Department.

DTIC sponsors the DoD Information Analysis Centers (IACs), which provide critical, flexible, and cutting-edge research and analysis to produce relevant and reusable scientific and technical information for acquisition program managers, DoD laboratories, Program Executive Offices, and Combatant Commands. The IACs are staffed by, or have access to, hundreds of scientists, engineers, and information specialists who provide research and analysis to customers with diverse, complex, and challenging requirements.

The Homeland Defense & Security Information Analysis Center (HDIAC) is a DoD IAC sponsored by DTIC to provide expertise in eight technical focus areas: alternative energy; biometrics; chemical, biological, radiological, & nuclear (CBRN) defense; critical infrastructure protection; cultural studies; homeland defense & security; medical; and weapons of mass destruction. HDIAC is operated by SURVICE Engineering Company under contract FA8075-21-D-0001.

A chief service of the DoD IACs is free technical inquiry (TI) research, limited to 4 research hours per inquiry. This TI response report summarizes the research findings of one such inquiry jointly conducted by HDIAC.

ABSTRACT

The Homeland Defense and Security Information Analysis Center (HDIAC) was asked to provide lessons learned in the ongoing conflict between Ukraine and Russia. These lessons should apply to both the strategic and tactical levels of combat. The inquirer requested that the research focus on studies from organizations like Federally Funded Research and Development Centers. HDIAC identified lessons in five overarching areas—tactics, unmanned aerial systems/drones, cyber and information warfare, military materiel, and space.

Contents

List of Figures

1.0 TI Request

1.1 INQUIRY

Can you provide a listing of studies/analyses on lessons learned from the Ukraine War with Russia?

1.2 DESCRIPTION

The inquirer requested a listing of current studies on lessons learned from the ongoing conflict between Ukraine and Russia. The focus was on the tactical and operational level of the conflict. The inquirer asked that research begin with studies from Federally Funded Research and Development Centers (FFRDCs) and similar organizations.

2.0 TI Response

The Homeland Defense and Security Information Analysis Center (HDIAC) began by searching all available FFRDC documentation. HDIAC also searched the unclassified Joint Lessons Learned Information System (JLLIS). Although results from JLLIS were limited, a document referencing several other studies was found. In reviewing these studies, preference was given to more recent studies that included lessons learned from the largest duration of the conflict. Early studies and reports were not necessarily discredited, but events in the conflict transpired in such a way that many early reports contained moot points.

An open-source search was also conducted, and results were filtered to focus on technological lessons learned. The key findings of the research will be outlined first, followed by a listing of pertinent documents and brief summaries from each.

2.1 KEY FINDINGS

2.1.1 Tactical Lessons Learned

- Unmanned aerial system (UAS)/drone use is rapidly growing and evolving.
- Although tanks are sometimes considered obsolete in modern warfare, their failure in the current conflict can be attributed to factors like poor command and control, logistical failures, and a lack of combined arms attacks. These factors have made tanks vulnerable.
- Rotary wing aircraft have been exceptionally vulnerable.
- Russian propaganda worked better on Russian troops than on Ukrainians. Russian troops expected little resistance and to be treated as liberators.

2.1.2 UASs/Drones

- The use of drones and other unmanned systems has been well documented, but the true effects and long-term sustainability may not be realized for some time.
- Drones are primarily used for intelligence, surveillance, and reconnaissance (ISR) and offensive missions.
- These were critical in the defense of Kyiv in the early months of the conflict.
- Commercial drones played a major role, particularly DJI drones.

2.1.3 Cyber and Information Warfare

- Although Russia possesses a robust cyber capability, they do not use it offensively the way it was predicted.
- Russian cyber capabilities are used more for information operations and espionage.
- Although Russia has experts in artificial intelligence (AI) many of these experts fled (although some returned) for fear of being pressed into service.
- Sanctions may reduce Russia's ability to purchase or manufacture new hardware, but efforts are already underway to circumvent the sanctions.
- Open-source intelligence is critical, including social media posts. Russian soldiers are being targeted when they violate rules and use their cell phones.
- Ukrainian political leaders used social media to communicate directly with their people.

2.1.4 Military Materiel

- Tanks have proven their relevance in this theater.
- Russia did not exercise solid combined arms tactics, leading to a lack of infantry to protect tanks. Coupled with poor logistics, this led many tank crews to abandon their tanks.
- Military-grade drones are in short supply. Both sides are relying on impromptu use of civilian drones, which can be more easily replaced. However, they are not hardened, physically or electronically, for military use.
- Rotary wing aircraft have been vulnerable.
- Munitions are being used up quicker than anticipated, including the High-Mobility Artillery Rocket System, javelins, stingers, and 155-mm artillery shells.

2.1.5 Space

- Ukraine has made use of allies' space-based ISR assets.
- Commercial space will grow in importance.

2.2 SUMMARIES OF RELEVANT DOCUMENTS

2.2.1 Center for Naval Analyses (CNA)

“A Technological Divorce: The Impact of Sanctions and the End of Cooperation on Russia’s Technology and AI Sector” [1]

This report from CNA explains what impact the international sanctions have had on the Russian technology sector. Although the impacts on the battlefield are not direct nor immediate, they will surely be felt when Russia exhausts its supply of hard disks and computer memory devices. There are some ways to work around the sanctions. For example, a Russian citizen could buy the devices in their country of origin and then transport them into Russia themselves. However, this is not sustainable in the long term.

“Russian Military Autonomy in Ukraine: Four Months In” [2]

Among autonomous systems being employed by both sides, the greatest impact is from UASs. Both sides have employed various military UASs, which are hardened physically, to the rigors of combat, and electronically (see Figure 1). The Russian military uses a wide variety of UASs, with the Orlan-10 the most widely used. Ukrainian forces are using the Turkish-made Bayraktar TB2 combat drone.

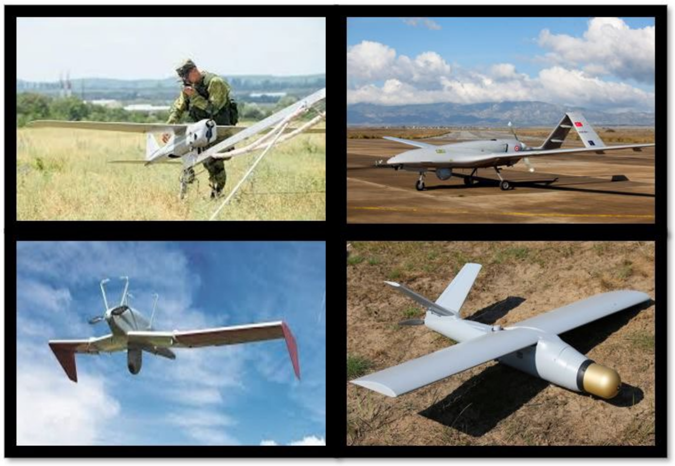

Figure 1: Russian Orlan-10 (Top Left), Turkish Bayraktar (Top Right), Israeli Bird Eye 400 (Bottom Left), and Polish Warmate (Bottom Right) (Source: U.S. Army Training and Doctrine Command).

While the report lists many other UASs which have been employed by both sides, a significant combat multiplier is the emergence of commercial UASs. In particular, the DJI Mavic drone has been used by both sides, primarily for ISR. Despite the drones’ lack of combat hardening, their economy and ease of use offsets this drawback. Ukraine has successfully used commercial drones to target Russian armored vehicles, hardened locations, and command and control points.

On the ground, there has been very limited use of unmanned demining vehicles by Russian forces, but the bulk is still being conducted by personnel. This report found no evidence of any type of maritime autonomous systems.

"Impacts of the Ukraine War on Russian Technology Development" [3]

The war has caused an outflow of Russian AI experts. Many have subsequently returned, but there will likely be an impact to autonomous systems being employed against Ukraine. Sanctions have caused shortages of other critical technologies, resulting in challenges to the Russian defense sector.

2.2.2 War on the Rocks

"The Tank Is Not Obsolete, and Other Observations About the Future of Combat" [4]

Tanks continue to play a critical role in modern combat, despite many saying that their role is reduced or obsolete. The fighting in Ukraine, as well as the recent war in Nagorno-Karabakh, demonstrated the significant contribution of tanks. Russia has suffered heavy losses in tanks, leading many to surmise that this was due to ineffectiveness of tanks. However, there are three issues which contributed to Russian tank losses.

First, a lack of warning and preparation caused tank crews and tank commanders to make untrue assumptions about the nature of combat they would face. Because they expected little resistance from the Ukrainians, they did not expect to use their tanks to fight. Therefore, their tactical employment on the front was poor. Second, poor strategy exacerbated logistics issues. Tanks routinely outran fuel supplies. Third, the Russian military has not employed tanks with sufficient infantry to be mutually supportive. Tanks and infantry must operate together—the infantry protects the tanks from antitank, man-portable weapons, land mines, and improvised explosive devices, and the tanks protect the infantry from armor or other infantry operating in hardened positions. Russia failed at this.

While antitank weapons play a role, the main killer of tanks in the Ukrainian war has been artillery. The Russian military has not coordinated the multiple domains of fighting well, despite Russian military training focusing on combined arms employment.

In the end, the most common cause of a Russian loss of a tank was crew abandonment. This was often caused by the lack of fuel. Many recovered Russian tanks have had little or no damage.

"The Other Big Lesson the U.S. Army Should Learn From Ukraine" [5]

The following three major lessons are cited in this article:

1. Open-source intelligence is playing a much bigger role in the fighting in Ukraine, more than ever in history. Social media posts, smartphone photos, drone videos, and cheap commercial satellite imagery have combined to provide an unprecedented view of the battlefield.
2. Rotary-wing aircraft are increasingly vulnerable in modern warfare when complete air supremacy is not achieved.
3. Security Force assistance programs have paid dividends and allowed the United States to better prepare Ukrainian forces for an attack. The National Guard's State Partnership Program has been particularly effective in aiding Ukraine. Figure 2 shows a multinational after-action review, which includes personnel from the California National Guard and Ukraine.

Figure 2: Leadership representatives from Canada, Georgia, Italy, Poland, Ukraine, and the California National Guard conduct an after-action review to conclude their portion of Rapid Trident 17 at the Simulation Centre on 21 September 2017 (Source: U.S. Army).

2.2.3 Breaking Defense

"US Army Secretary: 5 Lessons From the Ukraine Conflict" [6]

Secretary of the Army Christine Wormuth publicly spoke about the following lessons learned by the U.S. Army from the Ukraine conflict:

- Leadership on the battlefield matters.
- Logistics is a key combat enabler.
- Reduce electronic signature and the danger of cell phones.
- Prepare to defend against drones.
- Keep munitions stocked.

2.2.4 Royal United Services Institute (RUSI)

"Preliminary Lessons in Conventional Warfighting From Russia's Invasion of Ukraine: February - July 2022" [7]

Among many lessons learned and explored in this report from RUSI, the most important are provided.

The Russian military has proven that it is possible to carry out long-range precision strikes deep within enemy territory. Intelligence must be actionable and, most importantly, timely. Any friction points within the kill chain will cause unnecessary delays.

Stockpiles of weaponry, ammunition, and equipment must remain high in peacetime. The warring nations are depleting stocks much quicker than anticipated. Western nations supplying Ukraine are also depleting their stocks rapidly, bringing them down to what is considered minimum acceptable levels for a contingency. See the next article from the Defense Post regarding U.S. artillery supplies.)

UAS and counter-UAS equipment must be available across all branches of service and at all echelons of command in modern warfare. Electronic warfare (EW) is also critical, but the experience in Ukraine has refined some assumptions. It will not be possible to deny the electromagnetic spectrum across a large geographic area for a long period of time; this can be easily countered. EW can be used to sow confusion, slow kill chains, and deny precision weaponry.

Units, including air, must be able to disperse as much as possible to limit the enemy's weapons effects. They must also dig in or harden their targets both physically and in the cyber realm.

2.2.5 The Defense Post

"US Ammunition Supplies Dwindle as Ukraine War Drains Stockpiles" [8]

U.S. stockpiles of some munitions are reaching the lowest allowable levels. Ammunition usage has been much higher than expected for this kind of conflict. The United States has delivered 800,000 rounds of 155-mm shells, and production only stands at 14,000 per month. While there are plans to increase production of 155-mm shells, this could take years to be fully realized. The United States has delivered over 8,000 Javelin missiles, while producing only 1,000 per year.

2.2.6 The New York Times

"Artillery Is Breaking in Ukraine. It's Becoming a Problem for the Pentagon" [9]

The United States has provided M777 Howitzers to Ukraine. They are wearing down quickly as Ukrainian forces fire thousands of shells per day. A repair facility has been set up in Poland to replace barrels and provide other repairs. When the barrels wear down, this reduces accuracy. Ukrainian forces are engaging Russian targets at long range. This increases the need for propellant, thus increasing heat in the barrel and wearing the barrels more quickly.

2.2.7 Global Engagement Center

"Ukraine and the Power of 'We'" [10]

Russian messaging has not had a major effect on the front lines. Russian messaging tends to target its own people at home and abroad. Messaging is not generally targeted at foreign nationals like Ukrainian citizens. Russia's main message has been the idea that Russians and Ukrainians are "one people." However, atrocities undercut this message.

2.2.8 Carnegie Endowment for International Peace

"Cyber Operations in Ukraine: Russia's Unmet Expectations" [11]

Russia's Information Operations Troops remain in their infancy and appear optimized for counterpropaganda as opposed to offensive cyber operations. Russia's premier offensive cyber capabilities are focused primarily on intelligence and subversion rather than combined-arms warfare.

2.2.9 Small Wars Journal

"Commercial Drones/Robotics and the Modern Combat Zone: A Look at Ukraine" [12]

This report gives some specific examples of UAS/drone use, commercial and military, in the current conflict in Ukraine. In the early stages of the war, when Kyiv was threatened, the government called for people to use their personal drones in defense of Kyiv. When a 40-mile-long Russian convoy approached Kyiv, both the Ukrainian military and civilians used drones to monitor and attack the convoy.

Israeli Harpo drones have been used by Ukraine to fly and target autonomously. Sophisticated Russian counterdrone technology has failed to counter Ukrainian drone usage.

2.2.10 Organization for Economic Co-operation and Development

"Disinformation and Russia's War of Aggression Against Ukraine: Threats and Governance Response" [13]

This report outlines many of Russia's tactics regarding disinformation. Russia employs a vast network of human internet trolls and bots to spread disinformation. The report explains that 75 Russian government Twitter accounts, with millions of followers, tweeted 1,157 times from

25 February to 3 March 2022. Of these tweets, 75% covered Ukraine, and many furthered disinformation narratives. Also, Russian government accounts have typo squatted, which is where a common occurring typo of a domain is registered as its own domain. In the case of the Russians, they have typo squatted a page and made it look like the legitimate page but spread disinformation on the false page.

Shortly after the invasion, a Russian regulatory agency announced that media organizations could only receive information from official government media outlets on the war. They also declared investigations into outlets for disseminating unreliable information to the public. Clearly, the Russian government was attempting to gain full control of the narrative.

Meanwhile, Ukrainian leaders used social media to effectively communicate with their citizens. This allowed them to counter some of the Russian narrative.

2.2.11 Atlantic Council

"Early Lessons From the Russia-Ukraine War as a Space Conflict" [14]

Four major lessons regarding space conflict. First, Ukraine is using foreign space assets to prosecute their war. Second, antisatellite weapons have not been used by Russia, though they have attacked in the cyber domain. Third, commercial space assets will only increase in importance in the future. And fourth, Russia is not gaining a great advantage from their space assets, demonstrating its long-term weakness.

REFERENCES

[1] Gorenburg, D., A. Fink, S. Bendett, and J. Edmonds. "A Technological Divorce: The Impact of Sanctions and the End of Cooperation on Russia's Technology and AI Sector." Center for Naval Analyses, https://www.cna.org/reports/2022/04/A%20Technological-Divorce-The-impact-of-sanctions-and-the-end-of-cooperation-on-Russias-technology-and-AI-sector.pdf, accessed 25 January 2023.

[2] Bendett, S., and J. Edmonds. "Russian Military Autonomy in Ukraine: Four Months In." Center for Naval Analyses, https://www.cna.org/reports/2022/07/russian-military-autonomy-in-ukraine-four-months-in, accessed 25 January 2023.

[3] Fink, A. "Impacts of the Ukraine War on Russian Technology Development." Center for Naval Analyses, https://www.cna.org/our-media/indepth/2022/07/impacts-of-the-ukraine-war-on-russian-technology-development, accessed 27 January 2023.

[4] Lee, Rob. "The Tank Is Not Obsolete, and Other Observations About the Future of Combat." War on the Rocks, https://warontherocks.com/2022/09/the-tank-is-not-obsolete-and-other-observations-about-the-future-of-combat/, accessed 27 January 2023.

[5] Barno, D., and N. Bensahel. "The Other Big Lessons That the U.S. Army Should Learn From Ukraine." Was on the Rocks, https://warontherocks.com/2022/06/the-other-big-lessons-that-the-u-s-army-should-learn-from-ukraine/, accessed January 27 2023.

[6] Eversden, A. "US Army Secretary: 5 Lessons From the Ukraine Conflict." Breaking Defense, https://breakingdefense.com/2022/06/us-army-secretary-5-lessons-from-the-ukraine-conflict/, accessed 27 January 2023.

[7] Zabrodskyi, M., J. Watling, O. V. Danylyuk, and N. Reynolds. "Preliminary Lessons in Conventional Warfighting From Russia's Invasion of Ukraine: February - July 2022." Royal United Services Institute, https://pixtoday.net/article/file/2861123, accessed 27 January 2023.

[8] The Defense Post. "US Ammunition Supplies Dwindle as Ukraine War Drains Stockpiles." https://www.thedefensepost.com/2022/10/10/us-ammunition-supplies-dwindle/, accessed 27 January 2023.

[9] Ismay, J., and T. Gibbons-Neff. "Artillery Is Breaking in Ukraine. It's Becoming a Problem for the Pentagon." *The New York Times,* https://www.nytimes.com/2022/11/25/us/ukraine-artillery-breakdown.html, accessed 27 January 2023.

[10] Global Engagement Center. "Ukraine and the Power of 'We'." https://e.america.gov/t/ViewEmail/i/96785DB5309B7A402540EF23F30FEDED/8B82EB625026CDAFF039C523302FD418?alternativeLink=False, accessed 27 January 2023.

[11] Wilde, G. “Cyber Operations in Ukraine: Russia’s Unmet Expectations.” Carnegie Endowment for International Peace, https://carnegieendowment.org/2022/12/12/cyber-operations-in-ukraine-russia-s-unmet-expectations-pub-88607, accessed 27 January 2023.

[12] Edwards, B. “Commercial Drones/Robotics and the Modern Combat Zone: A Look at Ukraine.” *Small Wars Journal,* https://go.intelink.gov/rpRYHdA, accessed 27 January 2023.

[13] Bacio Terracino, J., and C. Matasick. “Disinformation and Russia’s War of Aggression Against Ukraine: Threats and Governance Response.” Organization for Economic Co-operation and Development, https://www.oecd.org/ukraine-hub/policy-responses/disinformation-and-russia-s-war-of-aggression-against-ukraine-37186bde/, accessed 27 January 2023.

[14] Burbach, D. T. “Early Lessons From the Russia-Ukraine War as a Space Conflict.” Atlantic Council, https://www.atlanticcouncil.org/content-series/airpower-after-ukraine/early-lessons-from-the-russia-ukraine-war-as-a-space-conflict/, accessed 27 January 2023.

BIOGRAPHY

John Clements is the technical lead for the Homeland Defense and Security Information Analysis Center. He served 20 years in the United States Marine Corps Reserve as a Combat Engineer. He deployed three times to Iraq in support of Operation Iraqi Freedom. His prior work includes test and evaluation on procedures and systems related to chemical, biological, radiological, and nuclear decontamination; mortuary affairs; cyber-insider threat; open-source and social media information; the common operational picture used by combatant commands; and the mounted computing environment. He has extensive experience working with joint, interagency, and allied partners at the strategic and tactical levels. Mr. Clements holds an M.A. in homeland security from the American Military University.