On Investing in Ukrainian Software

Open an office in Kyiv, but focus on the non-kinetic.

JAMES HASIK
RESEARCH NOTE
12 JULY 2023

A series of essays over the past few weeks, from leading technologists and industrialists, have led me to four points about the meaning of software in modern warfare:

1. Software has been eating the world, and as the Russo-Ukrainian War shows, it is now eating the war.

2. Software is different, and military bureaucracies in much of the world are still struggling with that reality.

3. The Ukrainians now know military software like no one else in the world.

4. In the long run, the Ukrainians will rule much of this business, so industry in North American and the rest of Europe should start working with them now. The two easy answers are to open an office in Kyiv, but for now, to focus on non-kinetic applications.

———

Software is eating the war.

As Marc Andreessen famously wrote in 2011, “software is eating the world.” Every large company had effectively become a software company, as software was so important to every company. Andreessen has recently and fortunately gotten interested in international security, for as I paraphrased him in 2014, “software is eating the war.” Many of the great military exploits of the Russo-Ukrainian War have been enabled by software, often recently written on the very front lines. We have learned how, as Jason Weiss and Dan Patt entitled their long study last year, “software defines tactics.” Software increases the value of even old military hardware, Alena Kudzko and General Pavel Macko wrote for the GLOBSEC think tank, by providing speed and precision for decision-making, particularly in the modern hider-finder competition. Even an old howitzer can become much more lethal if the crew better knows at what to shoot.

The ongoing Russo-Ukrainian War is revealing a particular Ukrainian genius for utilization of information, through masses of data, abundant connectivity, and user-friendly interfaces. All are frequently lacking in US systems. According to Schuyler Moore, the chief technologist for US

Central Command, “spotty networks and inadequate data” are the two chief obstacles to wider American use of artificial intelligence in military systems (reporting by Edward Graham). Even when connectivity is good, it can be targeted, and smart adversaries know this. Thus argued Heather Penney in a Mitchell Institute paper, modern military forces need not so much Christian Brose’s kill chains, but interconnected kill webs. Importantly, as Michèle Flournoy noted at the Atlantic Council’s Nexus 2023 conference this past May, we are beginning to see selective use of artificial intelligence for greater resilience in command and control, with intelligent, automated routing of communications traffic in self-healing wireless nets. That is essential in a world of warfare in which forces fight for information dominance.

Software is different.

As Elisabeth Gosselin-Malo wrote recently, progress in military robotics seems endlessly painfully slow. Like so many, but more so, robotics is a substantially software-defined industry. So why do we see such faster progress with software-driven command-and-control? After all, as Michael Kofman of the Center for Naval Analysis put it at Nexus, “rigid command-and-control is allergic to new technology.” The Russians really have that problem, but plenty of other militaries, if to lesser extent. Ah, Mohar Chatterjee pined in *Politico* last month, if the Defense Department could just get out of its own way in pursuing artificial intelligence applications. The problem is hardly endemic to the United States. As Ukrainian Defense Minister Oleksii Reznikov acknowledged in an essay for the Atlantic Council last week, old-school Soviet working styles are still afflicting Ukraine.

If the problem is hardly endemic to any one country, the problem is at once harder and easier with information systems. Ben Jensen, Christopher Whyte, and Scott Cuomo argue in a recent book that for adoption of new information systems, two factors particularly matter for military organizations: high or low resonance with existing ideas, and bureaucratic structures closed or open to innovation. Kudzko and Macko’s old howitzer provides the example. Fitting click-and-shoot tablet technology into artillerists’ kill webs makes for an easier marketing problem than outfitting every rifle platoon with first-person-view killer drones. As I noted in my essays of 29 June (“On Brilliant Munitions”) and 6 July (“On the Military, Demography, and Human Capital”), the marketing pitch to necessarily conservative military customers is easier when the functions are supporting. Making the howitzer crew more responsive and accurate resonates with conservative military understandings of what artillery is supposed to be and do. Then, if the change is isolated to the command-and-control system, a lesser fraction of the bureaucracy needs to come around.

Saliently, the production problem also differs. As a distinguished team at the US Defense Innovation Board entitled their study in 2019, *Software Is Never Done*. Software, they wrote, is “made by people, and for people, so digital talent matters.” As Kudzko and Macko wrote, this calls for “well-rounded development teams that include engineers, data analysts, military users, and ethics experts.” Field-user involvement is essential, because “products are never final, and can be constantly improved upon even after their adoption.” Indeed, they improve rapidly through use in the field, so “dragging out concept development over many years [just] produces suboptimal outcomes.”

Ukraine knows software.

The Americans have been quite bad at this until recently, taking too many cues from hyper-vigilant bureaucrats with *berührungsangst* about industry. Fighting an existential war, the Ukrainians have had no time for such silliness. Their "organized mess" of development is reminiscent of Israel, as Dima Adamsky has studied at length, with whatever-works interest in getting kit into the field. As with Iron Dome, so with tiny drones. From Ukraine, we should continue to expect Israeli-quality innovation, from another heavily armed front-line country constantly beset by crazy neighbors. As Timothy Hoyt wrote, sometimes states "peripheral" to the international security system produce world-class military innovations, simply because they must. As Kudzko and Macko wrote, the economics of software mean that "smaller conventional forces can gain an even greater marginal return on investment on these capabilities." That is because, as Eric Schmidt wrote in the *Wall Street Journal* this month, just "ten programmers can change the way thousands of soldiers operate." Perhaps then, as Seth Cropsey argued in the same newspaper a month earlier, masses of old-fashioned weapons may save Taiwan—if their crews can just get the targeting information.

Ukraine is showing the way. As Sebastien Roblin wrote in a long article for *Inside Unmanned Systems*, Ukraine already has a serious drone-industrial complex, with about 90 firms building military drones inside the country, benefiting from constant and rapid feedback from the front. As Schmidt noted, Ukraine's military drones are procured not primarily by the Defense Ministry, but by the Digital Ministry. Decision-making about which drones to use and how to use them has been devolved to the individual brigades and lower. As Kudzko and Macko noted, this has been enabled by a Ukrainian model of production that adjusts dual-use existing solutions, and leverages a technology-savvy military force and population. Indeed, as Shyam Sankar wrote in the *WSJ* in March,

> *Ukrainian conscripts are connoisseurs of software. They have a visceral knowledge of how it is built. Crucially, they have the vocabulary to provide feedback that can help developers improve the product. Their knowledge and experience has laid the foundation for collaboration among allied international software developers looking to help. In other circumstances, I'd be trying to hire them as engineers.*

So hire Ukraine.

As Eric Chewning and colleagues at McKinsey wrote last year, the entire US arms industry is lacking in software talent. In the short run, Chris Martin wrote in *Defense News* this week, the Russo-Ukrainian War "could reshape the global arms market in favor of China". Such a result would be good neither for American and European security or industry. As Kudzko and Macko put it, throughout NATO, this may not call for a state of emergency, but definitely a state of urgency. In the long run, militaries and industries to the west have reason to bet on Ukraine—indeed, to hire Ukraine as part of their value chain. As Defense Minister Reznikov argued,

> *Ukraine's entire defense doctrine should be underpinned by solid economic foundations. At present, the Ukrainian defense industry is not capable of meeting the demands of the*

military, but the sector has huge potential. Indeed, if managed correctly, a highly profitable Ukrainian defense industry could realistically become a major engine driving the country toward the goal of a one trillion dollar GDP.

Where Ukrainian talent and experience is matched with American investment and scale, great things have already happened. As T. X. Hammes has argued, Starlink, digital mobile governance, and Palantir's artificial intelligence software have provided Ukraine with military systems "probably already better than what the US is building." Ukraine is thus a place where American and European industrialists and investors should bet on software. I see at least two ways forward, in the short run.

First, open an office. First, as Byron Callan noted this week, maybe we should not too strongly lament low rates of research and development spending at US military contractors. At least several of them, notably led by Lockheed Martin, have been putting meaningful money into venture investing—and without necessarily consolidating those startups. Any number of military contractors can open offices in Kyiv or elsewhere around Ukraine to begin learning more about what is happening, what is possible, and whom to work with.

Second, focus on the non-kinetic. Those staffing the field office can then choose those easier tasks. Kudzko and Macko argued that those to the west should "pool collective resources" when investing in new software. One problem is that obtuse and cumbersome arms export rules, particularly in the US, make that challenging. This suggests what my former colleague Adam Thierer calls permissionless innovation, or just downright evasive entrepreneurship. Investing in digital governance, resilient communications, and automated logistics is not trafficking in a "munition". In a small-war context, this means building today the "technical"—the digital equivalent of the pickup truck—and fitting the weapon down the line, when the military situation demands it. Wait for the call, with the prints and software ready to go.

References and Further Reading

Adam Thierer, *Evasive Entrepreneurship and the Future of Governance*, Cato Institute, 2020.

Adam Thierer, *Permissionless Innovation: The Continuing Case for Comprehensive Technological Freedom*, Mercatus Institute, George Mason University, 2016.

Alena Kudzko and Pavel Macko, *The Future of Digital Deterrence in Central and Eastern Europe*, Bratislava: GLOBSEC, July 2023.

Ben Jensen, Christopher Whyte, and Scott Cuomo, *Information in War: Military Innovation, Battle Networks, and the Future of Artificial Intelligence*, Georgetown University Press, 2022. See also the book launch video at the CSIS on 22 February 2023.

Byron Callan, "Defense Contractor R&D: Partnerships & Ventures Are Other Paths to Ingest Tech," Capital Alpha Partners, research note, 10 July 2023.

Chris Martin, "Russia's war could reshape the global arms market in favor of China," *Defense News*, 10 July 2023.

Christian Brose, *The Kill Chain: Defending America in the Future of High-Tech Warfare*, Hachette, 2020.

Dima Adamski, *The Culture of Military Innovation: The Impact of Cultural Factors on the Revolution in Military Affairs in Russia, the US, and Israel*, Stanford University Press, 2010.

Edward Graham, "What's Holding Up the US Military's Use of AI?" *Defense One*, 28 April 2023.

Elisabeth Gosselin-Malo, "The military robots are coming — at some point," *Defense News*, 16 July 2023.

Eric Chewning, Matt Schrimper, Andy Voelker, and Brooke Weddle, "Debugging the software talent gap in aerospace and defense," McKinsey & Company, July 2022.

Eric Schmidt, "The Future of War Has Come in Ukraine: Drone Swarms," *Wall Street Journal*, 7 July 2023.

Heather R. Penney, *Scale, Scope, Speed & Survivability: Winning the Kill Chain Competition*, Mitchell Institute Policy Paper no. 40, May 2023.

J. Michael McQuade and Richard M. Murray, Gilman Louie, Milo Medin, Jennifer Pahlka, and Trae Stephens, *Software Is Never Done: Refactoring the Acquisition Code for Competitive Advantage*, US Defense Innovation Board, 21 March 2019.

James Hasik, "Software is Eating the War," *Defense Industrialist*, Atlantic Council, 3 November 2014.

Jason Weiss and Dan Patt, *Software Defines Tactics: Structuring Military Software Acquisitions for Adaptability and Advantage in a Competitive Era*, Hudson Institute, December 2022.

Marc Andreessen, "Why Software Is Eating The World," *Wall Street Journal*, 20 August 2011.

Mohar Chatterjee, "The Pentagon's endless struggle with AI," *Politico*, 27 June 2023.

Oleksii Reznikov, "Ukraine's defense doctrine will define country's future," *Ukraine Alert*, Atlantic Council, 7 July 2023.

Sebastien Roblin, "Adaptation at Hyper Speed: The Deadly Drone Arms Race in Ukraine," *Inside Unmanned Systems*, 14 June 2023.

Seth Cropsey, "Old-Fashioned Weapons Are a Key to Taiwan's Defense," *Wall Street Journal*, 2 June 2023.

Shyam Sankar, "Ukraine's Software Warrior Brigade," *Wall Street Journal*, 8 March 2023.

T. X. Hammes, at "Game Changers of Little Changed? Implications of Ground Combat in Ukraine," seminar, Atlantic Council, 3 April 2023.

Timothy D. Hoyt, "Revolution and Counter-Revolution: the Role of the Periphery in Technological and Conceptual Innovation," pp. 173-201 in Emily O. Goldman and Leslie C. Eliason, eds., *The Diffusion of Military Technology and Ideas*, Stanford University Press, 2003.