

Ukraine Aftershocks

Phillip Glen Armour , Corvus International Incorporated

Hal Berghel, University of Nevada, Las Vegas

Robert N. Charette , Ithabi Corporation

John Leslie King , University of Michigan

The major shock of the war in Ukraine draws attention to two aftershocks: asymmetric warfare and Ukraine's software outsourcing capability. Assessment of these provides a basis for additional speculation about the future of software.

“**A**ftershock” columns explore ideas with a combination of factual assessment and speculation. From this combination, we hope that evidence of important mechanisms of change will appear. This “Aftershock” column begins exploration of management guru Peter Drucker’s concept that knowledge will join, and possibly replace, traditional resources such as capital, land, minerals, and labor in enabling production. We examine the asset basis of the world and IT’s role in that.¹

The aftershock metaphor is that primary shockwaves trigger aftershocks that invite speculation. The goal is not to try to predict the future but to discern the patterns that suggest future scenarios. This article follows

this approach by taking the primary shock of the Russia-Ukraine conflict and examining two aftershocks: asymmetric warfare and software outsourcing. We make no claim that this is the best way to think about shocks or aftershocks, or, indeed, the ongoing conflict; but it is one. We also acknowledge, that as thinking moves away from factually grounded events, specula-

tion increases and predictions, when attempted, become less reliable. Nevertheless, speculation helps us construct scenarios that can be evaluated and that might eventually form the basis of planning.

PRIMARY SHOCK: THE RUSSIA-UKRAINE WAR

On 24 February 2022, Russia and Ukraine became engaged in an armed confrontation. Ukrainians call it unprovoked war. The Russian government has forbidden its citizens to use the word “war” to describe the conflict. The authors side with Ukraine on this. Arguably, this war began in 2014 with the Russian annexation of Crimea and instigation of insurrection in the Donbas region near the Ukraine-Russian border. Due to the nature of war and the aims of the combatants, it has been difficult in some cases to get reliable news from the conflict. But few who see the horrific images from

Digital Object Identifier 10.1109/MC.2022.3201212
Date of current version: 24 October 2022

Ukraine can doubt that a real war is underway. The Russia-Ukraine war is the primary shock that will frame the discussion that follows.

AFTERSHOCK 1: ASYMMETRIC WARFARE

For our purposes, there are two aftershocks following the primary shock of the Russia-Ukraine war. The first is the concept of “asymmetric warfare.” By this we mean kinetic war without weapons of mass destruction and where opposing sides have radically different levels of weaponry and resources. Asymmetric warfare has been

population and gross domestic product, and a much smaller army.

Reportedly, Russian leaders calculated that they would defeat Ukraine within a month. However, in large part because of their use of smart weapons—weapons often supplied by other countries opposed to Russia’s actions—Ukrainian forces were able to stop Russian advances in some areas, and even conduct successful counterattacks. Small, portable, and relatively inexpensive smart weapons have been used by Ukraine to destroy larger, more heavily armored and more costly Russian weapons systems. As evidence

Ukrainian forces have been able to transform an apparently dire situation using comparatively small and inexpensive “smart” weapons.

around for a long time. Throughout history, smaller and often less well-equipped combatants have sometimes been able to defeat large, sophisticated militaries. Guerilla movements can be successful because of the fierce intensity and resilience of their fighters even when the weaponry they use is quite simple. The Russia-Ukraine war is an example of such asymmetric warfare. Ukrainian forces have been able to transform an apparently dire situation using comparatively small and inexpensive “smart” weapons. These weapons leverage technology such that weaker adversaries can hold their own or even defeat more powerful adversaries. In subsequent assessment, we show how software is an exemplar of this. Such a sea change can upset a traditional predictor of military success: overwhelming force of arms. Stronger armed forces naturally have advantage over weaker adversaries. Bigger armies usually win. This imbalance in forces is evident in the current conflict. Ukraine is small compared to Russia, having roughly 4% of Russia’s land area, approximately 1/3 of its

of this, Ukraine appears to have sunk a major Russian warship in the Black Sea using a combination of drones and homegrown missiles. An essential and novel element of modern asymmetric warfare is its use of software. In part, this conflict is a David and Goliath story but with small, smart weapons in place of the sling.

The principles behind asymmetric warfare have been around for as long as humans have conducted wars. Asymmetry has been the way weaker powers defend themselves against stronger adversaries. Weaker powers have taken advantage of advanced weaponry, external support, terrain, and ideological passion to defeat stronger adversaries or make adversary’s victories costly. In recent memory, asymmetric warfare has occurred in Israeli-Palestinian conflicts, the Vietnam War, the wars in Iraq, and elsewhere. Over the centuries, asymmetric warfare has favored weaker defenders,² where the goal has been less to win than to avoid losing while gaining the time to get the upper hand through attrition or undercutting the enemy’s morale.

There are two takeaways from Ukraine’s asymmetric warfare story. One is that technology matters; it can give one party an advantage that, even if temporary, might be exploited in sufficient time to change the outcome. One way to consider this is the observe-orient-decide-act cycle, developed by military strategist John Boyd in the 20th century, which is now being applied to many challenges including cyberwarfare. Fast asymmetry can make it possible to operate inside the opponent’s decision loop to gain an advantage. The second takeaway is that willpower and resilience matter. Ukrainians are willing to take individual and collective risks that come from being the smaller, disadvantaged party. They use smart weapon technology at the “right time” to thwart the enemy. Software is a crucial factor in this technology.

AFTERSHOCK 2: SOFTWARE DEVELOPMENT OUTSOURCING

Ukrainian resilience also extends beyond the battlefield. Even while the conflict is ongoing, Ukraine’s software developers have continued to provide software outsourcing services to companies outside of their country. They have remained at work and are able to earn essential foreign currency to support their armed forces. It is clear that, at least in the area of software development outsourcing, Ukraine might be able to keep at least some economic activity going even while war rages. This is noteworthy. Historically, Ukraine has been known as an agricultural powerhouse, producing large quantities of wheat, sunflower oil, and sugar beets. Ukraine has almost one-third of the arable land in Europe. But it has not been generally known as a software outsourcing powerhouse. As recent events have shown, agriculture is easily threatened when transportation infrastructure is undermined. Ukraine agricultural exports were virtually shut off until the United Nations brokered a deal between Ukraine and

Russia to open the Port of Odesa and begin shipping food.³

Political and economic reforms take time but they also have an effect. Historically, Ukraine has faced persistent levels of poverty and corruption but was nonetheless characterized as an up-and-coming free market by the U.S. government’s International Trade Administration. However, according to the United Nations Development Program (UNDP), Ukraine has returned to poverty levels of 2004, losing 18 years of socioeconomic development. Moreover, a 2018 study by Credit Suisse ranked Ukraine 123rd out of 140 countries in terms of median wealth of its citizens, behind countries such as Bangladesh and Cameroon. Further, the German-registered nongovernmental organization Transparency International’s Corruption Perceptions Index (a measure of perceived levels of corruption in a country’s public sector) ranked Ukraine at 122 out of 180, where “1” represented the least corrupt and “180” the most corrupt countries according to the survey. Although Ukraine is dependent on aging Soviet-era infrastructure (for example, the Chernobyl Nuclear Power Plant), it has been growing in advanced manufacturing. Ukraine has produced automobiles, heavy trucks, ships, and aircraft, including the world’s largest commercial airplane, the Antonov AN-225. These and other technical advances have helped Ukraine create an entire software outsourcing industry.

Prior to February 2022, Ukraine’s macroeconomic trends were solidly improving. The World Bank records a more than 20-times reduction in poverty since a peak in 1996 (see Figure 1).

The expanding manufacturing base has been joined by a technology sector that has grown to US\$16.4 billion.⁴ This growth started in Soviet times, leveraging a strong educational system to produce an educated workforce. In 2021, universities and technical colleges added approximately 36,000 IT-related graduates to the economy per year—roughly the same number the

United States adds. Outsourcing of technology services to customers worldwide has grown substantially. These services are used by companies such as SAP, Grammarly, Fiverr, and Wix.com. An estimated 100,000 people worked in software development outsourcing⁵ in 2021.

The growth of software outsourcing in Ukraine has been assisted by market liberalization, which allowed business to grow organically. The limited in-country opportunities and availability of many educated software developers has led to outsourcing of software services to Western companies, particularly the United States. Such outsourcing has grown impressively,

from US\$4.2 billion in 2019 to US\$6.8 billion in 2021, as shown in Figure 2.

This growth required technical advances and evolution of an ecosystem to support remote, cooperative software development. High-speed Internet connections in primary development locations (Kyiv, Lviv, Kharkiv, Dnipro, and Odessa) as well as cloud-based services such as Amazon Web Services (AWS) and tools such as GitHub allow geographically independent development and storage of programs and data. The Starlink satellite communication system was added to this infrastructure.⁶ Open source software, project management, and application

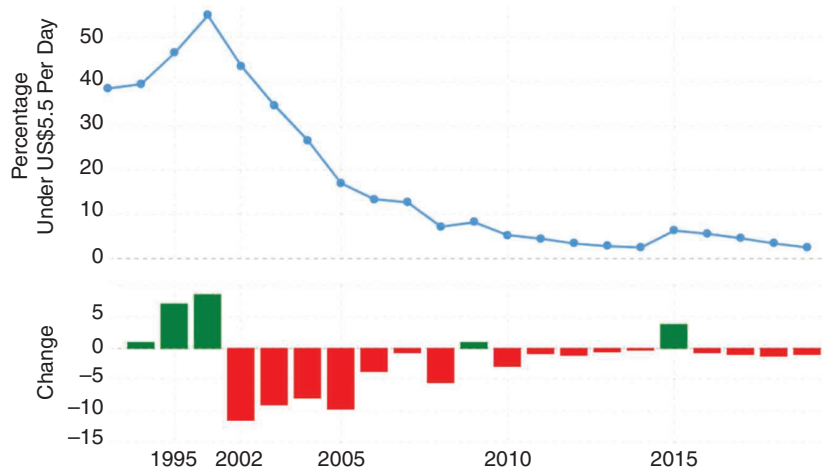


FIGURE 1. The reduction in poverty in Ukraine 1992–2019—people living on less than US\$5.50 per day. (Source: The World Bank, Poverty and Equity Data Portal.)



FIGURE 2. Growth in Ukrainian IT export services 2016–2020. (Source: IT Ukraine Association, 2021.)

of testing tools have helped outsourcing businesses minimize costs and incubate outsourcing start-ups.

This capability did not emerge overnight. A 2007 article discussed how an Evanston, Illinois, company outsourced software development to Ukraine.⁷ The article outlined necessary development environment elements that make software outsourcing across continents work. It emphasized the ecosystems needed by the company and their outsourcing partners to manage, specify, develop, test, and deliver software across the world. Such ecosystems are more prevalent now than they were in 2007. Time has also built expertise in such technologies. In addition to technical skills, Western business leaders have begun to notice and appreciate the diligence and honesty of Ukrainian developers and outsourcers. Although Ukrainian engineers are typically blunt in their assessments and opinions, they expect and produce high quality. They may not have been universally recognized, but some Ukrainian outsourcing companies have thrived for decades. The Ukrainian work ethic has also been supported by technical skills. In organizations, more than 90% of their

engineers are sourced from Ukraine's higher-education systems.

Many young engineers in Ukraine are fluent in the English language, which is a major advantage in working with global clients as English is the de facto lingua franca in IT. These language skills, coupled with technical prowess and growing business acumen, have created remarkable results according to one German-based outsourcing broker. Prior to the Russia-Ukraine conflict, Ukrainian engineers were launching start-ups at an impressive rate, with most focusing on providing outsourcing services to Western clients. To achieve this, they did leverage the advantage of relatively low-cost Ukrainian technical talent. But cost alone was usually not the deciding factor in acquiring business. A U.S. company that paid outsourcers from various countries and companies to produce sample applications from identical specifications was impressed. One executive noted that the Ukrainians "... simply blew everyone else away ...". This Ukrainian company got the job, and as the business relationship developed, the U.S. company increasingly viewed the Ukrainians not as hired hands, but as members of

their team. Similar experiences have been described by a number of U.S. and Western companies.

Circumstances sometimes motivate special expertise. Ukraine faced serious cybersecurity attacks aimed at disrupting its presidential election in 2014, and on its power grid in 2015, 2016, and 2017. The 2017 attack compromised radiation monitoring at the Chernobyl Nuclear Power Plant.⁸ Starting in 2022, fake SMS messages were broadcast to Ukrainians' phones, intending to sow panic in the population.^{9,10} The Ukrainian software development community was mobilized by these attacks and began to develop counter-capability. Even though most companies did not expect open warfare at scale, they did see a need to develop business contingency plans (BCPs) (see Figure 3).

NECESSITY IS STILL THE MOTHER OF INVENTION, BUT CONTEXT MATTERS

From Ukraine's perspective, the 2022 conflict started in 2014, when Russia annexed Crimea and instigated insurrection in the Donbas region near the Ukraine-Russian border. Companies began creating contingency plans, encouraging developers to update travel papers, putting together "go bags" of critical information and supplies, including necessary medicines. Every employee knew which other employees were vulnerable, what their family commitments were, which resources were available to families, whether families could and would relocate, and commitments that required families to stay. Transportation companies were contracted to be prepared to provide travel services on short notice. Dedicated fiber-optic lines were set up, lists of equipment to be moved made, and responsibilities assigned for oversight. Where prudent, servers were mirrored or relocated to neighboring countries such as Poland and Germany to preserve data. Outsourcing customers were informed of plans and possible interruptions, and how these would be handled.

Few expected that these measures would really be needed. Nevertheless,

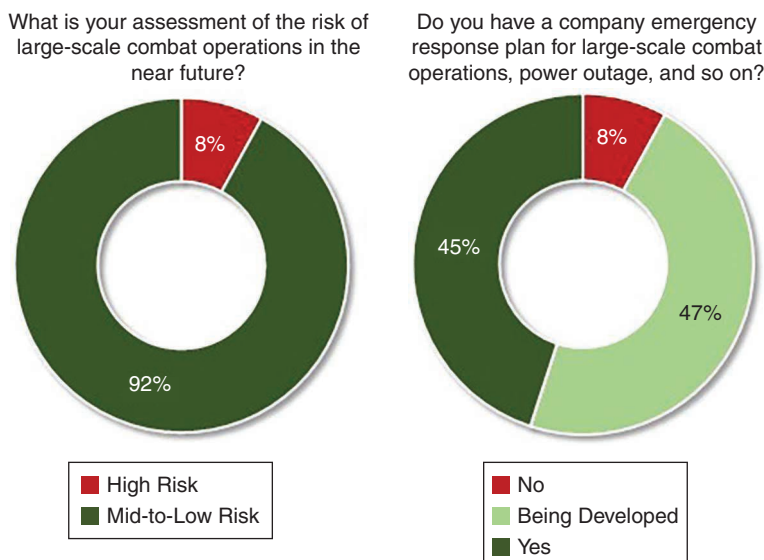
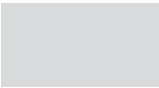


FIGURE 3. Ukrainian company conflict risk assessment and emergency response plan preparedness. (Source: adapted from IT Ukraine Association, February 2, 2022.)



following 24 February 2022, these “just-in-case” contingency plans were activated. Vulnerable employees in the east were relocated to the west. Some employees joined the Ukrainian defense forces while others stayed working for their clients. Families were provided assistance. Employees received cash advances on their salary to help tide them over. Buses were chartered and rail schedules distributed. Some outsourcing customer representatives from Western companies headed to Ukraine to help manage things. Conference calls with Ukrainian development teams initially were terminated at the sound of air raid sirens. Customers from around the world called their Ukrainian development partners to find out the impacts on deliverables and schedules, expressing their support for their Ukrainian partners and the Ukrainian people. These contacts brought home to many in the West what Ukraine was now facing.

Once the initial panic subsided, however, companies found that Ukrainian teams simply worked through alerts. Different conference call backgrounds showed that developers were moving to different locations for safety while they continued working their contracts. Many Western companies offered to continue funding their Ukrainian teams for months whether or not they produced deliverables and met deadlines. But, in large part, Ukrainians did meet their deadlines and did produce their deliverables. Disruptions were handled and families were taken care of. Some developers hunkered down and continued working. Some relocated, some fought. One Ukrainian engineer texted from northeast of Kyiv that once he finished working on an outsourcing task later that day, he would join the other fighters of the Territorial Defence Forces. Within a week, a Russian tank column attacked but was stopped just outside the city, its heavy losses forcing a retreat. The Ukrainian engineer from northeast of Kyiv has not been heard from since that time.

Almost paradoxically, the COVID-19 pandemic also played a significant role in preparing the Ukrainian software industry to continue functioning under these extreme circumstances. At a software outsourcing conference in Germany a few years before the outbreak of war, the CEO of a German-based outsourcing brokerage noted that, although Ukrainians were developing software for companies all over the world, they were still mostly working all together in small collocated offices; that developing systems for customers worldwide was mostly occurring with all the developers huddled together in one building seemed odd. It was largely a product of history, of course, when all the servers and workstations had to be in one place and all the people using them had to be in one place too. COVID-19 fixed

2022.¹¹ Groups as diverse as Microsoft, CrowdStrike, Ukraine’s “IT Army,”¹² and the hacker group Anonymous provided support to Ukraine in identifying and counteracting these attacks.¹³

Ukraine’s developers also actively fought back in a number of ways. Reface, an app that allows users to map their faces onto photographs and video clips of famous people, was used to push messages about the conflict worldwide. It used pictures of the Ukrainian flag, text messages describing the aggression, and slideshows of war images of bombed buildings and civilians sheltering in basements. Importantly, these messages were pushed to Reface’s 5.5 million Russian customers in an effective bid to bypass Russian censorship.¹⁴ A Kyiv digital app used to buy tickets for buses and pay for parking or utilities was modified

Reface, an app that allows users to map their faces onto photographs and video clips of famous people, was used to push messages about the conflict worldwide.

that. When the pandemic forced developers to disperse while continuing to work cooperatively, they learned to set up and use the necessary technology ecosystems. Aided by advances such as Internet-based conferencing, AWS, and Github, they also acquired the personal and interpersonal problem-solving skills that, when war struck, allowed them to uproot, relocate, continue serving clients, and continue earning money.

To continue working, Ukrainian developers have been aided by outside help from the Starlink system and other resources. They have maintained Internet connections despite cyberattacks originating in Russia and Belarus. The Ukraine Computer Emergency Response Team recorded more than 800 cyberattacks from five identified groups in the first quarter of

to give directions to bomb shelters, open pharmacies, and gas stations; it could also alert users to incoming air raids before the sirens sounded.^{15,16} An e-Enemy chatbot, working over the Ukrainian government’s Diia app, allowed citizens to inform the army when they saw Russian troop activity. Military intelligence began crowdsourcing evidence of war crimes.¹⁷

Despite the ongoing war, many Ukrainian outsourcing companies continue to grow their business, relocating within the country or, where necessary, to other countries. They are proving that the enormous technical and logistical challenges they are facing are surmountable. Ukrainians say they are culturally wired to accept, adapt, and overcome difficulties, and this is evident in the resilience of their IT infrastructure. Existing clients

continue to support business, despite the UNDP estimate of at least US\$100 billion worth of infrastructure destruction (buildings, roads, bridges, hospitals, schools, and so on) (see Figure 4). Many businesses have not been as resistant as software development and have been shut down. The conflict will severely increase poverty and limit the speed of economic recovery.^{18,19} Much Ukraine manufacturing and transportation infrastructure (rail, road, water) will have to be rebuilt. This will take a great deal of money and time.

In the short run, displaced refugees do need help. A lot of it. Ruined houses, villages, and cities must be rebuilt and the country's infrastructure reconstructed. Notwithstanding this immense damage, software development—a major and growing part of the economy—has continued to function. This capability is large enough to be a financial engine of reconstruction. Software development does not need immense infrastructure of roads, rail, and bridges; it needs only laptops, Internet connections, and special-purpose utilities (for example, cloud services and gits that coordinate

work among collaborative programmers).²⁰ And software development also needs smart and dedicated developers, of which Ukraine has plenty. As long as outside companies and countries continue sending work, it can funnel much-needed resources into the country.

Ukraine is not alone in providing software outsourcing services. Many countries, including India, the Philippines, and Poland, have mature software development capabilities and can leverage strong educational systems. They have lower average salary levels than many countries that need outsourcing help. Despite this highly competitive environment, software development provides a way forward for Ukraine. But even in countries considered safe from invasion and outright war, threats are always possible. Social, political, and military disruption can happen at any time, as can natural threats (hurricanes, tornadoes, typhoons, cold or heat waves). Nuclear, chemical, or biological accidents and adverse economic conditions can all threaten populations, wreck infrastructure, and diminish economic stability. Software outsourcing, although

unable to control events directly, can mitigate these challenges. IT must increasingly become part of any country's contingency plans for sustained economic security.

We see Ukrainians fighting for their country, culture, families, and future. They have been aided in this fight by technology in both society and weaponry. It is providing asymmetric warfare and economic competitive capability that has made their country more resilient than anticipated. As it appears to have happened with Ukraine it can be expected to happen elsewhere, changing the strategy and tactics of warfare. What is novel is the robustness of Ukraine's software industry, which is playing a major role in sustaining the country even as resources and infrastructure are being destroyed. Ukrainian economic stability requires the support of customers, companies, and countries in safer areas. In the words of one software developer: "Ukraine needs two things: weapons and work" Weapons to allow them to continue to execute effective asymmetric warfare against a much larger and well-armed adversary, and work to keep their economy

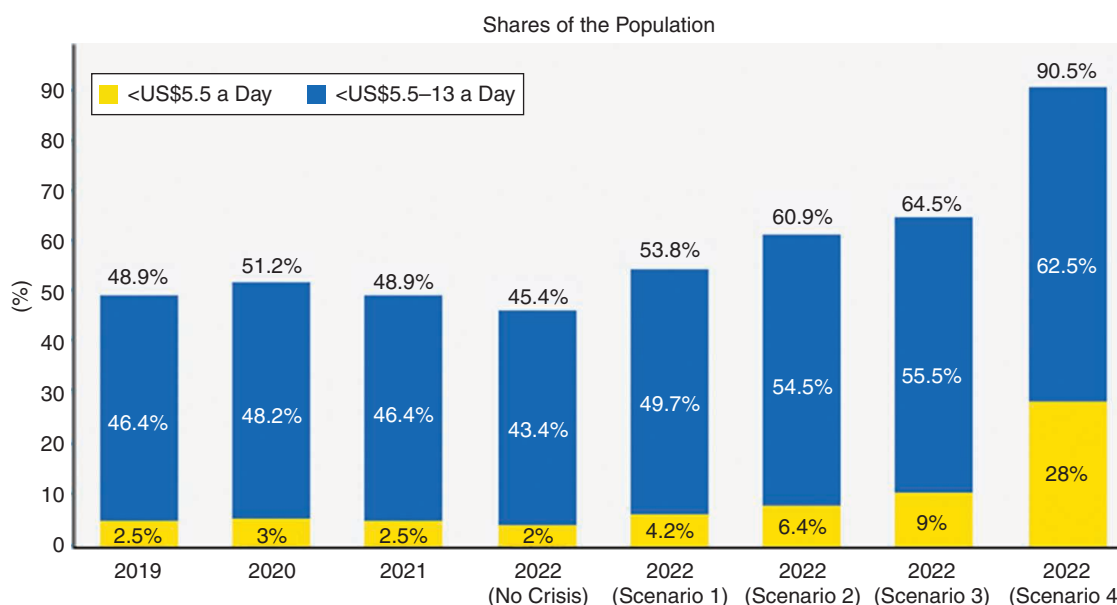


FIGURE 4. Percentage of the Ukrainian population living in, or vulnerable to, income poverty. (Source: UNDP: The Development Impact of the War in Ukraine, March 2022.)

going and to rebuild when the war is over. It is a powerful statement of IT's influence. But more powerful is a software outsourcing environment that can withstand disruption. The role of outsourcing causes us to consider other far-reaching issues involving IT in the nature of work and social power in the modern world.

STARTING TO CONNECT THE DOTS

An obvious dot is the role of that courage, resilience, and fortitude play in both asymmetric warfare and software outsourcing aftershocks. Even with a portable smart weapon that, properly used, can take out a tank, it takes a lot of courage for a foot soldier to go up against a tank. Similarly, the rapid formation and implementation of tactics that respond successfully to aggressive action by the enemy plays a big role in asymmetric warfare. It is fair to say that asymmetric warfare would be impossible without such attention, courage, and fortitude. All have been on display in Ukraine.

At the same time, all the attention, courage, and fortitude in the world cannot overcome a larger, and vastly more powerful, adversary. Asymmetric warfare requires technology that, properly used, confers a lethal advantage on whichever party uses it most effectively. Gaining this advantage might require attention, courage, and fortitude, but it also requires the technology necessary to prevail. In this, the smaller party might have an advantage where it is sufficiently agile to act more quickly than is possible for its adversary.

Both the effectiveness of the smart weapons being used on the battlefield and of the Ukrainian outsourcing industry are related. In the Second World War, the U.S. Army employed an antitank missile launcher known colloquially as a *bazooka*. This weapon is essentially a metal pipe into which a rocket with a shaped-charge warhead is placed. The gunner estimates the distance to a target, aims the bazooka, and fires. The knowledge of how to

perform these actions is retained as a printed version in the weapon manual, in the hardware calibration of the weapon and the missile's performance, and in the brain of the gunner. In the modern version of this system, most of the knowledge is retained in software in the weapon and the missile. The FGM-148 Javelin is an example. It has been extensively, and very effectively, used by Ukrainian armed forces against Russian armored col-

Periodically, we return to the guiding question: How does information and its processing come to be an essential factor in production of any stripe? It is not sufficient to say that it will happen. We are searching for the mechanisms by which it happens. Software outsourcing in Ukraine illustrates ecologies of workplaces that connect to people's lives. Examining aftershocks often exposes simple causal mechanisms: the underlying currents that are

The role of outsourcing causes us to consider other far-reaching issues involving IT in the nature of work and social power in the modern world.

umns. Although the warhead on such devices is what does the damage, the missile's targeting software-based targeting and guidance knowledge places the warhead where it can destroy the target. It is software, rather than explosive firepower, that makes the weapon truly effective. The Javelin is a fire-and-forget missile that allows the antitank team to fire at the target and relocate before countermeasures can trace the launch and retaliate. In the hands of an agile defensive force, this has proved highly effective.

Ukraine's special circumstances should be noted because they are globally relevant for the future. These, at least as appears now, bolstered Ukraine's ability to do software outsourcing work in a disruptive crisis. BCPs were drawn up because of early experiences with warfare that occurred before the invasion in early 2022. The COVID-19 pandemic forced software outsourcing workers to work remotely for extended periods of time, which in turn forced these workers to learn how to function cooperatively while staying up to date on shared project work. They could continue to get things done despite the disruptions that accompanied the war.

driving change in the modern world. Outsourcing may assume a simple mechanism of wage arbitrage, that is, cheaper labor replaces more expensive labor. But as seen in Ukraine, outsourcing has come to involve a whole host of things: attentiveness, courage, fortitude, technical and domain expertise, knowledge of how the right "inputs" become the right "outputs" in a large system, and so on. Ukraine's IT workers who work in software outsourcing understand such things. These IT workers are not necessarily fungible with other IT workers in one country or another or with one another. One set of developers may have the necessary combination of technical expertise, domain knowledge, thoroughness, and sometimes just plain grit, which means they are not easily replaced by others who, although being "cheaper" do not possess such attributes.

Initial software outsourcing ventures tend to be cost-driven with the work going to whoever offers to build the systems at the lowest cost to the client. Over time, however, Ukrainian developers have acquired specific development skills and application knowledge that their customers have come to rely on. These competencies

will likely provide a more solid basis for acquiring and retaining future work than simple low cost. Necessity is the mother of invention, but invention is the mother of necessity as well. One can certainly conclude that the war has made Ukrainians dependent on software outsourcing. But one can also conclude that the character of software outsourcing in Ukraine is dependent on the war. Being able to see this reciprocity is not just an important part of using Ukraine software outsourcing services effectively, it is important to seeing how the services “fit in” to the whole.

There is an underlying truth that is emerging, and it is evidenced by the enormous increase in software in modern society. As Peter Drucker noted in *Post-Capitalist Society*, production is always constrained by what he called the *limiting asset*. The limiting asset is that which determines whether any enterprise or production will be successful. In the distant past, this asset was land. People had to be fed, and growing crops or raising cattle required land; ergo, those in possession of land were extremely powerful and many wars were fought to acquire this asset. Building a powerful navy in the 19th century required the limiting assets of coal (or oil) and iron ore to make steel. Those countries that possessed these limiting assets in easily obtainable quantities were the powerful countries. When large-scale, continent-wide enterprises arose toward the end of the 19th and early-20th centuries, capital became the limiting asset. To build a railroad across a continent required people, to employ people required the money to pay them. So rich people, who were in possession of a lot of this limiting asset, became powerful.

Drucker asserted that the limiting asset of the modern world is not

land, oil, or cash, it is knowledge. That knowledge of how to manage supply chain, optimize equipment scheduling, predict failures in an oil rig, or land a warhead on top of a tank from two miles away is present these days in software systems. This knowledge is inserted into these systems by developers. Therefore, software developers are the mechanism by which the limiting asset of the modern world is created. Where ownership of land, mines, oil wells, or large quantities of cash used to confer power, now it is ownership of software development capability.

Drucker’s question about how knowledge becomes a part of the explanation of production receives two insights by this consideration of aftershocks from the primary shock of the Russia–Ukraine war. One is that knowledge informs labor. This is not a new insight; it reinforces something understood for many centuries: knowledgeable workers produce better results. Knowledge might play a role in capital, hard asset, and land management and transactions, but these assets are not themselves knowledge. Software production and assets are knowledge. But the second insight is more general, not tied just to labor, land, or capital. A “knowledge ecology” operates in nearly all situations, and it is possible that simpler situations have simpler ecologies. Figuring out simple ecologies might happen on the fly with knowledgeable workers. But as situations become more complicated, the knowledge is spread across mechanisms such as the relationships among workers and organizations, standards, curricula, and (in cases like Ukraine) the specialized knowledge “taught” by prevailing circumstances such as the Russia–Ukraine war.

If the past is a guide, our efforts to fathom the role of knowledge in production will cause us to re-examine things we previously considered understood. For example, capital, land, and labor might play roles in

production as essential as ever, but different from the past. Introducing something as fundamental as knowledge as an asset class does not simply change the list of variables, it changes the idea of what to include and the model of causality. On one hand, there is a temptation to leave this alone and go with earlier models. But on the other hand, people are resourceful, noticing when earlier models fail to handle certain circumstances and developing new ways of thinking about the future become more important. As IT (and particularly software) becomes more important, new ways of thinking about the future become more enticing.

In the future, we will build upon the primary shock of the Russia–Ukraine war and the aftershocks of asymmetric warfare and software outsourcing to explore scenarios of transformation. **G**

ACKNOWLEDGMENT

Phillip Glen Armour is the corresponding author.

REFERENCES

1. P. Drucker, *Postcapitalist Society*. London, U.K.: Routledge, 1993.
2. I. Arreguin-Toft, “How the weak win wars: A theory of asymmetric conflict,” *Int. Security*, vol. 26, no. 1, pp. 93–128, 2001. [Online]. Available: <https://web.stanford.edu/class/polisci211z/2.2/Arreguin-Toft%20IS%202001.pdf>
3. P. Polityuk, M. Hunder, and M. Nichols. “First Ukraine Black Sea grain shipments could move in days—U.N., Ukraine.” Reuters. Accessed: Jul. 25, 2022. [Online]. Available: <https://www.reuters.com/markets/commodities/ukraine-hopes-first-grain-shipment-under-un-brokered-deal-this-week-2022-07-25/>
4. “According to the US Government’s International Trade Association,” International Trade Administration U.S. Department of Commerce, Washington, DC, USA, 2022. [Online]. Available: <https://www.trade.gov/country-commercial-guides/ukraine-market-overview>

EDITORS’ NOTE

This and a subsequent article form a group.

5. "Ukraine's Booming tech outsourcing sector at risk after Russian invasion." Wall Street Journal. Accessed: Feb. 24, 2022. [Online]. Available: <https://www.wsj.com/articles/ukraines-booming-tech-outsourcing-sector-at-risk-after-russian-invasion-11645749755>
6. "Ukraine Leans on Elon Musk's Starlink in fight against Russia." Wall Street Journal. Accessed: Jul. 26, 2022. [Online]. Available: <https://www.wsj.com/articles/ukraine-leans-on-elon-musks-starlink-in-fight-against-russia-11657963804>
7. P. G. Armour, "Agile...and offshore," *Commun. ACM*, vol. 50, no. 1, pp. 13-16, Jan. 2007, doi: 10.1145/1188913.1188930.
8. "UKRAINE: Timeline of cyberattacks on critical infrastructure and civilian objects." CyberPeace Institute. Accessed: May 23, 2022. [Online]. Available: <https://cyberpeaceinstitute.org/ukraine-timeline-of-cyberattacks>
9. "CISA, FBI, and NSA release cybersecurity advisory on Russian cyber threats to U.S. critical infrastructure," Cybersecurity and Infrastructure Security Agency, Washington, DC, USA, Jan. 11, 2022. [Online]. Available: <https://www.cisa.gov/uscert/ncas/current-activity/2022/01/11/cisa-fbi-and-nsa-release-cybersecurity-advisory-russian-cyber>
10. "Alert (AA22-110A): Russian state-sponsored and criminal cyber threats to critical infrastructure," Cybersecurity and Infrastructure Security Agency, Washington, DC, USA, Apr. 20, 2022. [Online]. Available: <https://www.cisa.gov/uscert/ncas/alerts/aa22-110a>
11. "Five hacker groups that attack Ukraine the most," State Service of Special Communications and Information Protection of Ukraine, Kyiv, Ukraine, 2022. [Online]. Available: <https://cip.gov.ua/en/news/p-yat-khakerskikh-ugrupuvan-yaki-naichastishe-atakuyut-ukrayinu>
12. "According to a report in the Wall Street Journal, Ukraine's IT Army may have more than 400,000 volunteers assisting in cyber countermeasures against Russian actors and institutions." Wall Street Journal. Accessed: Mar. 4, 2022. [Online]. Available: <https://www.wsj.com/livecoverage/russia-ukraine-latest-news-2022-03-04/card/ukraine-s-it-army-has-hundreds-of-thousands-of-hackers-kyiv-says-RfpGa5zmLtvrot27OWX>
13. "In a report published by Yahoo!finance, the hacker group Anonymous leaked personal data of 120,000 Russian military personnel including dates of birth, addresses, passport numbers, and army unit assignments." Yahoo. Accessed: Apr. 4, 2022. [Online]. Available: <https://finance.yahoo.com/news/anonymous-takes-reveng-e-putin-brutal-185953836.html>
14. "Reface, a viral face-swap app from Ukraine, adds anti-war push notifications." Yahoo. Accessed: Feb. 27, 2022. [Online]. Available: <https://finance.yahoo.com/news/reface-viral-face-swap-app-195258511.html>
15. "Kyiv transport app is transformed into life-saving war information tool." Guardian. Accessed: Mar. 15, 2022. [Online]. Available: <https://www.theguardian.com/world/2022/mar/15/kyiv-transport-app-is-transformed-into-life-saving-war-information-tool>
16. "'We became like a big startup.' How Kyiv adapted the city's tech to save lives." Time. Accessed: Apr. 4, 2022. [Online]. Available: <https://time.com/6163708/kyiv-digital-technology-app/>
17. "A Citizen-like chatbot allows Ukrainians to report to the government when they spot Russian troops — Here's how it works." Business Insider. Accessed: Apr. 18, 2022. [Online]. Available: <https://www.businessinsider.com/ukraine-military-e-enemy-telegram-app-2022-4?op=1>
18. "Every day of delayed peace will accelerate a freefall into poverty for Ukraine, warns UNDP," United Nations Development Programme, New York, NY, USA, Mar. 16, 2022. Accessed: Mar. 10, 2022. [Online]. Available: <https://www.undp.org/press-releases/every-day-delayed-peace-will-accelerate-freefall-poverty-ukraine-warns-undp>
19. "The development impact of the war in Ukraine – Initial projections," United Nations Development Programme, New York, NY, USA, 2022. Accessed: Mar. 10, 2022. [Online]. Available: <https://www.undp.org/sites/g/files/zskgke326/files/2022-03/Ukraine-Development-Impact-UNDP.pdf>
20. "Git." Wikipedia. Accessed: Sep. 14, 2022. [Online]. Available: <https://en.wikipedia.org/wiki/Git>

PHILLIP GLEN ARMOUR is the director of the Corvus International Shields Lake Center for Leadership Development, Faribault, MN 55021 USA. Contact him at armour@corvusintl.com.

HAL BERGHEL is a Fellow of IEEE and ACM and a professor of computer science at the University of Nevada, Las Vegas, NV 89154 USA. Contact him at berghelnet@protonmail.com.

ROBERT N. CHARETTE is the founder of ITABHI Corporation and managing director of the Decision Empowerment Institute, Spotsylvania, VA 22551 USA. Contact him at charette@itabhi.com.

JOHN LESLIE KING is a W.W. Bishop collegiate professor at the School of Information, University of Michigan, Ann Arbor, MI 48109 USA. Contact him at jlking@umich.edu.