

# EDTs vo vojne na Ukrajine: príklady nasadenia

BRIEF č. 4, október 2023

Vojna na Ukrajine je **javiskom využívania a testovania nových technológií v ozbrojenom konflikte**. Hoci rozhodujúca je stále ťažká pozemná a letecká technika, nové technológie (EDTs) otvorili ďalší front vedenia a podpory vojenských operácií. Ukrajina nie je prvou krajinou, ktorá používa UAV, kybernetické nástroje boja, umelú inteligenciu, vesmírne spôsobilosti či hypersonické systémy. V predchádzajúcich konfliktoch však nebola zapojená taká široká škála týchto prostriedkov a neboli integrované do sofistikovanejších systémov.

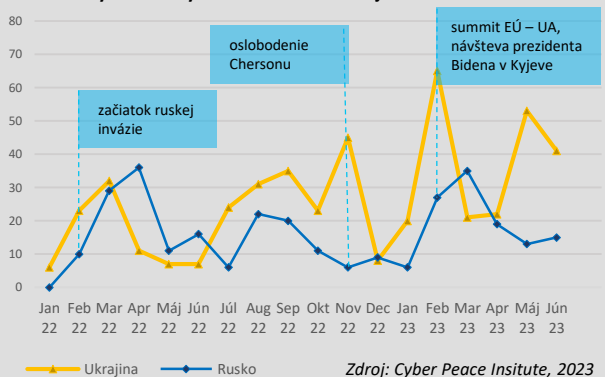
Okrem nových technológií sa v konflikte objavujú aj **noví aktéri s vplyvom na vedenie operácií**. Medzi nich patria súkromné spoločnosti, hacktívi, ale aj jednotlivci aktívni v online priestore. Príkladom je organizácia NAFO (North Atlantic Fella Organisation). NAFO využíva sociálne médiá a kultúru tzv. „memov“ na združovanie priaznivcov Ukrajiny z celého sveta, aby bojovali proti ruskej propagandistickej mašinérii, predovšetkým na Twitteri (X). NAFO sa zmočňuje ruských dezinformačných kont a spochybňuje nepravdivé tvrdenia ruských predstaviteľov. Skupina má aj serióznejšiu rovinu, ktorou je napr. podpora snáh o crowdfunding.

**Prepájanie nových technológií a nových aktérov významne ovplyvňuje vedenie operácií a vývoj konfliktu.**

**Príkladom významu tejto synergie je využívanie bezpilotnej techniky.** Najznámejšie sú v súčasnosti tzv. bojové drony, napr. turecký Bayraktar TB2 (nesie laserom navádzané bomby), v USA vyrobený Switchblade a ruský Lancet, tiež známy ako „kamikadze dron“. Aj keď sú vyššie spomínané drony vysoko účinné, ich cena je pomerne vysoká. Najbežnejšie bezpilotné prostriedky používané ukrajinskými vojakmi sú preto komerčné voľne dostupné drony, ako je Phantom 3 od DJI alebo Quantix Recon od spoločnosti AeroVironment. Majú integrované kamery s vysokým rozlíšením, ktoré možno spárovať so smartfónom. The Royal United Services Institute odhaduje, že Ukrajina mesačne stráca až 10 000 dronov, čo ilustruje rozsah ich využívania. Hoci sú tieto platformy decentralizované, snímky, ktoré zachytávajú, sa môžu agregovať do oveľa väčších súborov údajov, ktoré spolu vytvoria pomerne presný obraz o situácii na sledovanom území.



## ▼ Počet kybernetických incidentov na Ukrajine a v Rusku

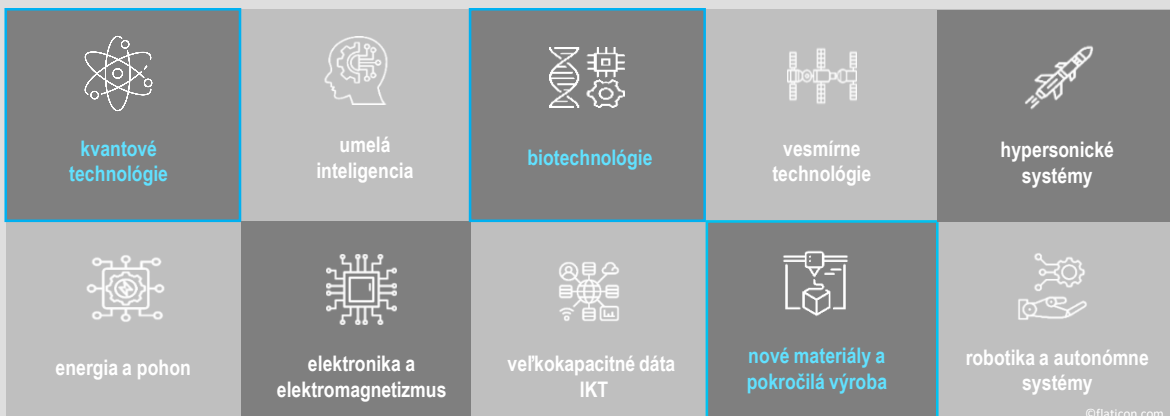


## ▼ Príklady zapájania globálnych technologických spoločností do konfliktu na Ukrajine

- ✓ **Amazon** dodal Ukrajine zariadenia „snehovej gule“ (počítačové úložné jednotky vo veľkosti kufru) na pomoc pri ukladaní a prenose údajov (do decembra 2022 pomohla presunúť približne 10 petabajtov údajov do cloudu, čo zodpovedá niekoľkým stovkám tisíc celovečerných filmov)
- ✓ **Google** rozšíril prístup k svojmu bezplatnému softvéru **Project Shield**, čím prispel k vytvoreniu „kybernetického dáždnika“, ktorý chráni ukrajinské webové stránky pred útokmi
- ✓ **Microsoft** poskytol prístup k svojim cloudovým službám, zatiaľ čo jeho centrum **Microsoft Defender Analýzy hrozieb** poskytlo správy sledujúce ruské dezinformácie a kybernetické útoky (podpora Ukrajine v rokoch 2022-23 bude mať odhadovanú hodnotu 400 miliónov dolárov)
- ✓ **SAP** - spoločnosť poskytla vlastné cloudové služby, softvérové licencie pre zbraňové systémy a prístup k **SAP Arriba Discovery** - službe, ktorá podporuje dodávky humanitárnej pomoci Ukrajine

Zdroj: Franke & Söderström, 2023 a Bohrn, 2023

EDTs (**emerging** and disruptive technologies) sú nové vedecké objavy a technológie a/alebo technológie vo fáze vývoja, ktoré ešte nedosiahli zrelosť, ale v oboch prípadoch existuje predpoklad, že budú mať revolučný vplyv na obranno-bezpečnostnú oblasť. Zriedkavo nahrádzajú existujúce technológie okamžite, spočiatku sú len čiastočne integrované do existujúcich plánov, doktrín a operácií. EDTs zmenili charakter vojny tým, že vytvorili nové vektory pre eskaláciu krízy, nové schopnosti na bojisku a vytvorili príležitosť pre nových aktérov zohrať kľúčovú úlohu v konflikte.



▲ EDTs podľa NATO STO, 2023 (deľba a definície EDTs sa naprieč organizáciami mierne líšia)

## 1. Veľkokapacitné dáta, informačné a komunikačné technológie a umelá inteligencia

<b>DELTA</b>	Označované aj ako „Google mapy pre armádu“. Poskytuje pohľad na bojisko v reálnom čase v súlade so štandardmi NATO prostredníctvom integrácie údajov z rôznych zdrojov vrátane leteckého prieskumu, satelitných snímok a záberov z dronov. Systém bol vyvinutý Inovačným centrom v rámci ukrajinského ministerstva obrany.
<b>KROPYVA</b>	Mapovacia spravodajská aplikácia na systéme Android, ktorá umožňuje osobe s terminálom, zvyčajne tabletom, jednoducho označiť nepriateľské postavenie. Softvér potom prenáša indikáciu na blízke delostrelectvo, pričom umožňuje koordináciu ich palby proti rovnakému cieľu z niekoľkých samostatných pozícií. Kropyva sa rovnako stáva nevyhnutným nástrojom pri odminovaní. Používa krátkovlnné a digitálne rádiové stanice kompatibilné s bezpečnostnými komunikačnými štandardmi NATO.
<b>eVOROG</b> (spustený v rámci aplikácie DIIA)	Chatbot, ktorý umožňuje zhromažďovanie spravodajských informácií. Chatbot dá používateľom zoznam otázok, aby zistil, čo videli, kde a kedy (na kontrolu identity odosielateľov využíva aplikáciu DIIA a funkcia satelitnej navigácie telefónu potvrdí polohu), následne sa informácia potvrdí prostredníctvom iných zdrojov (do decembra 2022 dostal viac ako 450 000 správ).
<b>PRIMER</b>	Softvér, ktorý pomocou AI umožňuje hlasový prepis a preklad za účelom spracovania zachytenej ruskej komunikácie a automatického zdôraznenia informácií relevantných pre ukrajinské ozbrojené sily vo forme textovej databázy s možnosťou vyhľadávania. AI tu umožňuje pracovať tempom, ktoré by si inak vyžadovalo stovky analytikov.
<b>CLEARVIEW AI</b>	Softvér, ktorý využíva rozpoznávanie tváre na vyhľadanie profilov zosnulých vojakov na sociálnych sieťach. Informáciu používajú úrady na informovanie príbuzných a odovzdávanie tiel rodinám.
<b>PALANTIR</b>	Americký softvér, ktorý pomáha Ukrajine zamerať nepriateľské tanky a delostrelectvo, pričom technológia umožňuje sledovať vývoj vojny v reálnom čase (na vizualizáciu pozícií armády využíva prevažne zdroje zo satelitov a sociálnych médií).
<b>SORM</b>	Ruský softvérový systém na sledovanie Ukrajincov a cenzúru ich spravodajstva. Systém bol tiež pravdepodobne použitý na potlačenie ruských aktivistov, ktorí vyjadrili nesúhlas s vojnou na Ukrajine, a v infraštruktúre v okupovaných častiach Ukrajiny s cieľom efektívnejšie integrovať ukrajinské územie do Ruska.
<b>SCALE-AI</b>	Americká firma využíva strojové učenie na analýzu snímok Ukrajiny. Ukrajinským silám pomáha pochopiť, kde k útokom dochádza a posúdiť škody rýchlejšie a presnejšie v porovnaní s ľudskými hlásením.
<b>ZVOOK</b>	Experimentálny systém, ktorý identifikuje a sleduje ruské nadzvukové rakety. Využíva na to zvukovú stopu týchto rakiet, ktorú identifikuje s použitím umelej inteligencie rýchlejšie ako bežný radar. Systém je v prototypovej fáze.

Na ruskej strane mal **projekt 22160** dodať námorníctvu hliadkové lode schopné monitorovať a chrániť moria s menšou posádkou vďaka automatizácii. Okrem toho ruská strana tvrdí, že používa AI v automatickom zameriavacom delostreleckom systéme (MSTA-SM) alebo protipečhotnej mine (POM-3 Medallion).

## 2. Vesmír

<b>STARLINK</b>	Komerčná vesmírna konštelácia zameraná na satelitnú komunikáciu, dopĺňa spôsobilosti poskytované vládnymi systémami. Na Ukrajinu bola nasadená po vyradení satelitnej siete KA-SAT, ktorú vlastní spoločnosť Viasat, po ruskom útoku. Poskytuje včasné spravodajské informácie o pohyboch ruských vojsk a udržiava ukrajinské vojenské komunikačné siete v prevádzke. Starlink čelil viacnásobným pokusom o neutralizáciu ruským elektronickým systémom Tobol.
<b>HAWKEYE 360</b>	Satelitná konštelácia o.i. zbiera a monitoruje rádiový signál rušenia GPS. Rádiový signál rušenia GPS sa využíva napr. na ochranu kritických vojenských jednotiek či zariadení a môže signalizovať blížiacu sa vojenskú aktivitu.

## 3. Hypersonické strely

<b>Avangard, Kinžal, Zirkón</b>	Na rozdiel od balistických rakiet, hypersonické strely (HGV alebo HCM*) nesledujú parabolickú trajektóriu. Strategická výhoda je v ich rýchlosti (nad Mach 5). Ďalšou výhodou je tzv. plazmový oblak (počas letu je raketa pokrytá plazmovým oblakom, ktorý absorbuje akékoľvek lúče rádiových frekvencií a robí raketu neviditeľnou pre radary). Na ceste k cieľu môžu manévrovať, čo sťažuje ich detekciu a zničenie. Rusko v súčasnosti podľa dostupných údajov disponuje tromi typmi takýchto striel: Avangard (HGV, odpaľované z ICBM, Mach 27), Kh-47M2 Kinžal (HCM, odpaľované zo vzduchu, napr. MiG-31, 2,7 - 10 Mach – na hrane hypersonických striel, vyvinuté pravdepodobne z rakiet Iskander) a 3M22 Zirkón (HCM, odpaľované z mora, Mach 9, experimentálne štádium).
---------------------------------	---

\* HGV – hypersonic glide vehicles, sú vypustené do vesmíru, potom sa vracajú do atmosféry, aby sa „kĺzali“ k cieľu; HCM – hypersonic cruise missile sú poháňané prúdovými alebo raketovými motormi počas celého letu

## 4. Robotika a autonómne systémy\*\* (UUV, UAV, USV)

<b>TOLOKA TLK-150</b>	Bezpilotné podmořské vozidlo (UUV) s technológiou stealth. Dron má vykonávať aktivity ako lokalizácia nepriateľských jednotiek na mori, zhromažďovanie spravodajských informácií alebo odhaľovanie mín. Je výsledkom ukrajinskej verejno-súkromnej obrannej spolupráce (Brave 1) a je prvým UUV, ktorý si vyvinula Ukrajina sama.
<b>VOLK-18</b>	Plne autonómny dron, ktorý sa využíva na ničenie nepriateľských UAV. V záujmovej oblasti dron autonómne hliadkuje a snaží sa lokalizovať UAV protivníka, k čomu využíva pasívny optický systém, povel k neutralizácii však naďalej zadáva operátor, neutralizáciu uskutočňuje dron opäť autonómne.
<b>SEA BABY</b>	Vytvorený na základe nemeckého podmořského dronu Seafox, ktorý je schopný samostatne dosiahnuť určený cieľ a detonovať, čo je využívaný pri odmiňovaní. Tieto drony inšpirovali ukrajinské bezpečnostné zložky k vytvoreniu vlastného námorného dronu Sea Baby, ktorý bol použitý napr. na zničenie Kerčského mosta.

\*\* Ukrajina urýchľuje proces obstarávania a zvyšuje domácu produkciu UAS dvoma paralelnými snahami:

1. **iniciatíva Army of Drones** (funguje na princípe darovania komerčných a vojenských dronov/financii/výcvik pilotov)
2. **odstránenie obchodných prekážok pre dovoz dronov** (DPH, colné bariéry aj pre dovoz náhradných dielov a komponentov)

## LESSONS LEARNED

- I. vesmír a kybernetický priestor potvrdené v praxi ako nové operačné domény vo vedení operácií
- II. popretie predstavy o vedení moderného konfliktu výhradne v kybernetickom priestore s nízkym počtom obetí
- III. vplyv sociálnych médií na šírenie/potláčanie propagandy a dezinformácií s vplyvom na vývoj konfliktu
- IV. súkromné technologické spoločnosti (výrobcovia dronov, firmy pôsobiace v oblasti AI, snímkovania, dátovej podpory, komunikačnej infraštruktúry) ako čoraz samostatnejší aktér a multiplikátor sily v konflikte
- V. nárast vplyvu „hacktivistov“ - kolektív hackerov, ktorí útočia na počítačové systémy z politických dôvodov (napr. tzv. „IT Armáda Ukrajiny“)

### Zdroje:

1. Bellasio, J. et al. „*Innovative Technologies Shaping the 2040 Battlefield*“. RAND Europe. 2021. [https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690038/EPRS\\_STU\(2021\)690038\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690038/EPRS_STU(2021)690038_EN.pdf)
2. Bernstein, P. & Menke H. „*Russia's Hypersonic Weapons*“. 2019. <https://gija.georgetown.edu/2019/12/12/russias-hypersonic-weapons/>
3. Bohrn, B. „*Four Tech Lessons Learned from the Ongoing War in Ukraine*“. 2023. <https://globaleurope.eu/europes-future/four-tech-lessons-learned-from-the-ongoing-war-in-ukraine/>
4. Cyber Peace Institute. „*Cyber Threats*“. 2023. <https://cyberconflicts.cyberpeaceinstitute.org/threats>
5. Favaro, M. & Williams H. „*False Sense of Supremacy: Emerging Technologies, the War in Ukraine, and the Risk of Nuclear Escalation*“. Journal for Peace and Nuclear Disarmament. 6:1. 28-46. 2023. DOI: 10.1080/25751654.2023.2219437
6. Fedorov, M. „*Tech innovation helps Ukraine even the odds against Russia's military might*“. 2023 <https://www.atlanticcouncil.org/blogs/ukrainealert/tech-innovation-helps-ukraine-even-the-odds-against-russias-military-might/>
7. Franke, U. „*Drones in Ukraine and Beyond: Everything You Need to Know*“. 2023. <https://ecfr.eu/article/drones-in-ukraine-and-beyond-everything-you-need-to-know/>
8. Franke, U. & Söderström, J. „*Star tech enterprise: Emerging technologies in Russia's war on Ukraine*“. 2023 <https://ecfr.eu/publication/star-tech-enterprise-emerging-technologies-in-russias-war-on-ukraine/>
9. Healey, J. „*Ukrainian Cyber War Confirms the Lesson: Cyber Power Requires Soft Power*“. 2023 <https://www.cfr.org/blog/ukrainian-cyber-war-confirms-lesson-cyber-power-requires-soft-power>
10. Jones, G. & Ergan, J. & Rosenbach, E. „*Advancing in Adversity: Ukraine's Battlefield Technologies and Lessons for the U.S.*“. 2023 <https://www.belfercenter.org/publication/advancing-adversity-ukraines-battlefield-technologies-and-lessons-us>
11. Jones, S.G. & McCabe, R. & Palmer A. „*Ukrainian Innovation in a War of Attrition*“. 2023. <https://www.csis.org/analysis/ukrainian-innovation-war-attrition>
12. Mações, B. „*How Palantir Is Shaping the Future of Warfare*“. 2023. <https://time.com/6293398/palantir-future-of-warfare-ukraine/>
13. NATO STO. „*Science & Technology Trends 2023-2043: Across the Physical, Biological, and Information Domains*“. 2023.
14. Palaveni, D. „*The Use of Emerging Disruptive Technologies by the Russian Armed Forces in the Ukrainian War*“. Air Land Sea Space Application (ALSSA) Center. 2022. <https://www.alsa.mil/News/Article/3170285/the-use-of-emerging-disruptive-technologies-by-the-russian-armed-forces-in-the/>
15. Slofer, W. „*Progress in hypersonics missiles and space defense. Cyber- Human Systems, Space Technologies, and Threats*“. 2023. <https://kstatelibraries.pressbooks.pub/cyberhumansystem/s/chapter/13-progress-in-hypersonics-missiles-and-space-defense-slofer/>
16. Sutton, H.I. „*Innovative Submarine Drone Is Ukraine's New Weapon Against Russian Navy*“. 2023 <https://www.navalnews.com/naval-news/2023/05/innovative-submarine-drone-is-ukraines-new-weapon-against-russian-navy/>
17. Taylor, D. „*Despite the War, Ukrainian Smart Home Startup i3 Engineering is Growing in Europe*“. 2023. <https://tech.eu/2023/02/24/despite-the-war-ukrainian-smart-home-startup-i3-engineering-is-growing-in-europe/>
18. The Economist. „*How a chatbot has turned Ukrainian civilians into digital resistance fighters*“. 2023. <https://www.economist.com/the-economist-explains/2023/02/22/how-a-chatbot-has-turned-ukrainian-civilians-into-digital-resistance-fighters>
19. Wang, B. „*Russia military official claims mach 8 Zircon hypersonic missile is operational*“. 2017 <https://www.nextbigfuture.com/2017/11/russia-military-official-claims-mach-8-zircon-hypersonic-missile-is-operational.html>
20. Werner, D. „*HawkEye 360 detects GPS interference in Ukraine*“. 2022. <https://spacenews.com/hawkeye-360-gps-ukr/>

© Analytický útvar MO SR, október 2023

Kútuzovova 8  
832 47 Bratislava

Web: [www.mosr.sk/au-mosr/](http://www.mosr.sk/au-mosr/)

Autor: Dagmar Schönová

Ed. Barbora Hrozenšá

Materiál prezentuje názory autora a Analytického útvaru MO SR, ktoré nemusia nevyhnutne odzrkadľovať oficiálne názory a politiky Ministerstva obrany SR. Cieľom komentárov a iných materiálov AÚ je podnecovať a zlepšovať odbornú a verejnú diskusiu na aktuálne témy v oblasti obrannej a bezpečnostnej politiky štátu. Práca neprešla jazykovou úpravou. Za spracovanie rešerše ďakujeme p. Pavlovi Beblavému.