CYBERDEFENSE REPORT

The Ukrainian Way of Digital Warfighting

Volunteers, Applications, and Intelligence Sharing Platforms

Stefan Soesanto

Zürich, July 2024
Center for Security Studies (CSS), ETH Zürich

CSS
ETH Zürich

ETH zürich

Available online at: https://css.ethz.ch/en/publications/risk-and-resilience-reports.html

Author: Stefan Soesanto

ETH-CSS project management: Stefan Soesanto, Project Lead Cyberdefense; Andreas Wenger, Director of the CSS.

DOI: 10.3929/ethz-b-000685245

Table of Content

Executive Summary

Aerorozvidka's history and its development of Delta is deeply intertwined with Ukraine's way of digital warfighting in response to the Russian invasion of 2022. Aerorozvidka was founded in the aftermath of the Maidan revolution and amidst the ongoing war in Donbas. The group was the first to experiment with drones on the Ukrainian battlefield and it was the first to deploy stationary cameras – equipped with satellite internet uplinks – on high-rise building for military situational awareness purposes. With Aerorozvidka's integration into the Ukrainian Armed Forces as Unit A2724, the group became the technical hub for all soft- and hardware products used by the Ukrainian military. As such, it built relationships with numerous volunteer groups to create and implement technical solutions for the military's problems.

The origin of Delta goes back to the 2014 NATO Wales Summit and the creation the NATO-Ukraine C4 Trust Fund. The Fund's goal was to move Ukraine's communication, command and control, and computing systems (C4 for short) toward a concept known as network centric warfare. In other words, enhancing situational awareness to outmaneuver a much later enemy army. Delta evolved from the Fund's Situational Awareness Project, which also ensured NATO interoperability. As part of the Fund's Knowledge Sharing Project, the Delta team participated in several NATO Tide Sprints, NATO Tide Hackathons, and the alliance's annual Coalition Warrior Interoperability eXploration, eXperimentation, eXamination, eXercise (CWIX). In October 2022 – eight months after the Russian invasion – Delta was officially unveiled during NATO's Tide Sprint 2022 in Virgina Beach, USA.

Delta's first deployment on the battlefield occurred almost immediately after the invasion during the defense of Kyiv in February/March 2022. Much of Delta's success was reliant on the shipment of Starlink terminals to Ukraine in the aftermath of the ViaSat hack. Starlink allowed units to be mobile on the battlefield and directly upload sightings of Russian troop movements and stream a drone's video feeds directly into the Delta platform for the headquarters to analyze. Headquarters were also able to view sector and battlefield-wide developments in almost real-time and could make immediate decisions to concentrate forces and engage Russian targets. Delta essentially enabled Ukrainian Armed Forces to operate with 21 century command-and-control infrastructure, while its military assets and equipment were still stuck in Soviet times.

To underpin the success of Delta, Aerorozvidka NGO deployed nine situational centers across the frontline oblasts. The center's missions are to enrich the Delta platform with information provided by partner nations (i.e. satellite imagery), walk-in informants, video-feeds from stationary cameras and other sources. Meanwhile, intelligence cells receive a constant flood of targeting information (Russian troop movements, warehouses, artillery positions, helicopter pads, etc.) directly from Ukrainian civilians via the eEnemy and Stop Russian War Telegram bots, as well as the Bachu mobile application. All that information is directly fed into the Delta platform to enhance situational awareness and provide units with decision-making advantages. As of this writing, Ukraine has been so innovative that even Western militaries have not articulated how they would adapt if future adversaries would replicate Ukrainian efforts to crowdsource military intelligence en masse via mobile applications.

The importance of Delta for Ukraine's way of digital warfighting has likely also changed the way Russian hacktivists, cybercriminals, and nation-state actors are operating. Meaning, every Delta user, their loved ones, connected devices, Starlink terminals, and communication streams are of interest to breach the Delta platform. To protect Delta, the Ukrainian government even made the unusual step to allow the platform to be deployed on a cloud server outside of Ukraine. As of this writing, no international cloud provider nor foreign government has publicly entertained the idea of hosting Delta on their territory.

Studying the success of Aerorozvidka and tracing the evolution of Delta is synonymous to understanding the Ukrainian way of digital warfighting. It provides a window to grasp how a military can adapt to new technologies and possibilities, and how innovative ideas can be integrated and nurtured. Some of these innovations are not in line with the laws of armed conflict, such as the publication of prisoner of war videos and the involvement of civilians to gather military intelligence. But maybe, what Ukraine is showing the world is how a war ought to be fought in the digital age. Maybe Delta – or the lessons of Delta – will be exported and emulated across the globe which will create new challenges for how modern militaries will operate from here on out. With Delta still evolving and Aerorozvidka continuing to innovate, we will likely witness the further integration of robotics and development of autonomous system that will turn heads in the not-so-distant future. Understanding what is happening in Ukraine, is understanding where modern warfare is heading toward, and what we need to prepare for in the age of digital warfighting.

This CSS Cyberdefense report puts forward four specific recommendations:

1. Western militaries and policymakers must think about how they can mobilize their own expat communities abroad. Particularly those that work in the areas of IT, journalism, marketing, and fundraising activities. Western militaries must also think about how to create ad-hoc relationships across all their domestic talent pools – including veterans, pensioners, university/high school students, and walk-in volunteers. Depending on the conflict scenario at hand, mobilizing the global IT community might also be a distinct possibility which will necessitate active engagement and political narrative shaping.

2. Western governments would do well to figure out what third-country software products used for war can – or should not be allowed to – be hosted on cloud servers located on their territory. A comprehensive legal analysis might be necessary to identify classification criteria, regulatory loopholes, and company transparency requirements.

3. Of particular value for the replication debate would be a legal analysis on how and whether the Ukrainian government's implementation of eEnemy – i.e. interfacing with both the official Ukrainian e-government app (Diia) and the country's premier military situational awareness platform (Delta) – is in line with international humanitarian law.

4. Cyber scholars and think tankers would do well to focus their research on electronic warfare and the intersection of cyber and EW – also known as CEMA (cyber electromagnetic activity). Rather than just viewing cyber as an isolated stand-off capability, the reality on the Ukrainian battlefield is moving toward overlapping mission requirements and tactical integration. Russian cyber operators working side-by-side with special operations forces and electronic warfare officers is where the innovation of cyber in war is at.

Introduction

The Ukrainian military situational awareness platform Delta (Дельта) is at the heart of this CSS report. Initially developed in 2015 by Aerorozvidka (Аеророзвідка – then military unit A2724), the platform is currently owned, maintained, and upgraded under the auspices of the Center for Innovation and Development of Defense Technologies within the Ukrainian Ministry of Defense (Центром інновацій та розвитку оборонних технологій Міністерства оборони України).

Starting from the war in Donbas in 2014 to the Russian invasion in 2022, the origin and evolution of Delta provide a near perfect case study to trace the development of digital warfare thinking in Ukraine. For this CSS cyber defense report, Delta serves as the red thread to introduce to the reader a host of digital platforms, mobile applications, and Ukrainian volunteer groups that helped to shape Delta. As the war in Ukraine has entered its third year, the story of Delta provides a window into Ukraine's miltech revolution. This report provides analysts, researchers, and policymakers with a comprehensive understanding as to (1) what opportunities and stumbling blocks volunteer groups had to overcome in their bottom-up push for change, (2) why and how Aerorozvidka pushed for the adoption of a concept known as 'network-centric warfare', and (3) how Russia has reacted to Ukraine's digital warfighting efforts.

The report's focus on digital warfare encompasses primarily systems and applications that deal with information generation and dissemination. This spans from mobile applications used to transmit data on incoming Russian air breathing threats to platforms designed for orientation and situational awareness on the kinetic battlefield. Academic literature does not necessarily distinguish between the term digital warfare and cyber warfare. They are broadly considered to mean the same thing. While this report has no intention of creating new definitions, for the author the term digital warfare encompasses a three-step process: (a) generating data and information from various intelligence sources, (b) using digital applications and platforms to store, process, and disseminate said data and information, and (c) utilizing these applications and platforms to make tactical decisions on the kinetic battlefield. Digital warfare thus describes the digitalization of the kinetic battlefield (i.e. information and data enrichment and sharing). This definition stands in stark contrast to the term cyber warfare, which can be narrowly defined as conducting offensive cyber operations against adversarial digital systems. Net-

work-centric warfare is the conceptual idea on how to utilize digital warfare products so that they can unfold their potential and help increase combat power. That being said, digital warfare is tied to cyber at the hip. As the kinetic battlefield is becoming increasingly digitalized, cyber threat actors from across the spectrum naturally pivot to target these systems – particularly during an ongoing international armed conflict. This can encompass anything from transmitting false data and information, breaching applications and platforms, and disseminating fake ones. This report will thus also in part cover the cyber component to Ukraine's digital warfighting.

Chapter one explains the circumstances as to who, why, and how Aerorozvidka was founded. What activities the group conducted on the battlefield and why they were eventually absorbed into the Ukrainian Armed Forces as unit A2724. In two sub-chapters, the reader will also be introduced to the history and impact of (a) ArmySOS and their proprietary software product Kropyva, and (b) Eugene Maksymenko's ComBat Vision.
Chapter two dives into the development of Delta and why it was moved into the Center for Innovation and Development of Defense Technologies. It explains Delta's origin within the NATO-Ukraine C4 Trust Fund and the importance of the alliance's Tide Hackathons for the development of Delta until its release at NATO's TIDE Sprint 2022 in Virginia Beach, USA. It also explains Delta's fallout with the Ukrainian company Everest.
Chapter three informs the reader about the activities of Aerorozvidka NGO, including the functioning of its situational centers and the importance of Starlink for the wide adoption of Delta in in the aftermath of the ViaSat hack.
Chapter four explains what cybersecurity measures have been implemented by the Center for Innovation and Development of Defense Technologies and Aerorozvidka NGO to protect Delta and its users. It also highlights significant cyber- and information warfare incidents conducted by a variety of hostile actors to breach and discredit the platform.
Chapter 5 introduces to the reader an assortment of mobile applications that feed crowdsourced intelligence data and information into the Delta platform.
Chapter 6 informs the reader about the Terminal system, which functions similarly to Delta and was also first deployed during the defense of Kyiv in February 2022.
Chapter 7 dives deeper into the impact of the ViaSat hack. Explaining the significance of Ukrainian satellite reseller Datagroup and highlighting the importance of satellite internet access for specific application such as GIS Arta. Chapter 7.2 briefly discusses the relationship between GIS Arta and the Ukrainian charity foundation Coma Back Alive, and the latter's role in supporting Ukrainian offensive cyber operations.
Chapter 9 concludes the report with an assortment of further thoughts.

Research Methodology

This report is solely based on open-source intelligence and non-classified data. Sources include newspaper articles, blogs, Twitter and Facebook posts, Telegram channels, YouTube videos, LinkedIn lookups, threat intelligence reports, as well as live and archived websites. All social media posts referenced in this report have been backed-up on either the Wayback Machine or archive.today.[1] Google Translate and DeepL were used for all language translations from Ukrainian and Russian to English.

The digital applications mentioned in this report were chosen because they (a) feed data directly into Delta, or (b) provide further context as to what other applications are actively used on the battlefield in Ukraine. For example, Kropyva and Combat Vision were chosen because of their working relationship with Unit A2724. And ePPO was of particular interest due to its simplicity and significant impact. The focus on ViaSat in the latter third of the report was necessary to highlight (a) the importance of ViaSat/Datagroup to GIS Arta, and (b) the significance of Starlink to Delta.

To avoid any potential biases and accidental revelations of non-public – or potentially still classified – data amidst the ongoing international armed conflict in Ukraine, no individuals were interviewed for this report. The author did not seek access or any special insights into the digital platforms and applications discussed. Nor did he request any technical details, specifications, or other information that might aid belligerents in the war in Ukraine.[2] The report does not make any legal, ethical, or moral judgements when it comes to Ukraine's way of digital warfighting.

[1] Note: Archive.today is the only service that correctly archives Telegram and Facebook posts. By contrast, the Wayback Machine is a hit or miss as it very often returns archiving failures or non-results when trying to archive social media posts.

Please also note that as of this writing, archive.today is still stuck in an ongoing dispute with Cloudflare's DNS service, which is why the website might not correctly dissolve for you. Alternatively, instead of using archive.ph, please replace the link with archive.is, archive.md, or archive.vn. Using a different browser or opening the link on your mobile phone might also help resolve it correctly.

[2] The author did approach Aerorozvidka once by email to ask where the photo in figure 1 was taken, and whether Aerorozvidka would be willing to disclose the identity of some of the individuals in the photo which the author was unable to identify. Aerorozvidka disclosed that the picture was taken in November 2014 at Yavoriv and that the man standing next to Nathan Khazin is Oleksandr Kyvatkovski.

1 Aerial Reconnaissance

Aerorozvidka was created in July 2014, during the war in Donbas – Ukraine's most eastern region bordering Russia. Four individuals founded the group: Volodymyr Kochetkov-Sukach, Nathan Khazin, Yaroslav Gonchar, and Dmytro Lisenbart.[3] Volodymyr Kochetkov-Sukach was essentially the leader of Aerorozvidka [engl. Aerial Reconnaissance]. As Dmytro Lisenbart put it, "the idea of [creating Aerorozvidka] was suggested by Volodymyr Kochetkov, nicknamed 'Chewbacca,' who had already been in the [war in Donbas]. Vova was the main carrier of the ideology, and he was the flagbearer of [Aerorozvika]. He promoted it everywhere he went. In the General Staff, in the field, in companies, and in some brigades. There were times when Vova would come in and out of the tent, and the commanders would say, 'well, probably some general, who the hell knows, we have to do everything the guy said.' And they did."[4] Dmytro Lisenbart fought at the Maidan and is the artistic member of the group. As an animator and film director, he designed Aerorozvidka's first logo and likely disseminated his technical knowledge of digital cameras within the group. Nathan Khazin, briefly served in the Israeli Defense Forces, and was part of the Jewish Hundred, a neighborhood defense force that fought on the Maidan in 2014.[5] Among others, the Jewish Hundred cooperated with the ultra-nationalists Right Sector, Maidan Self-Defense, and Automaidan – which Yaroslav Gonchar belonged to.[6]

To understand the relationship between Nathan Khazin and Yaroslav Gonchar we must go back to May 5, 2014, when the Azov Battalion – Ukraine's controversial far-right volunteer paramilitary militia – was formed. Azov started out as an umbrella organization that loosely united under its roof multiple Ukrainian groups that fought on the Maidan. Among them the aforementioned Right Sector, the Jewish Hundred, Maidan Self-Defense etc. During Azov's early days, the Russian invasion of the Donbas and Crimea posed such an existential threat to the Ukrainian homeland that these distinct groups forced each other to work together despite their clear ideological differences. This resulted in Jews fighting side-by-side with neo-Nazis, and anarchists working together with Orthodox Christian nationalist. The incorporation of the Jewish Hundred into Azov made Nathan Khazin one of the co-founders of the Azov Battalion. With the inclusion of Automaidan, Yaroslav Gonchar became one of Azov's deputy commanders.[7] The loose unity and underlying ideological friction within Azov, led to constant infighting, position reshufflings, and inconsistent information sharing within the group as well as externally.

For Khazin and Gonchar the trouble fomented when they – together with the 72nd mechanized brigade of the Ukrainian Armed Forces – fought a Russian insurgency in Mariupol during the Victory Parade on May 9, 2014.[8] The investigation into the battle's aftermath, and particularly Gonchar's operation to free Oleksiy Serheyev, the then head of the election headquarters of former Prime Minister Yuliya Tymoshenko, resulted in Azov interrogating, torturing, and expelling Gonchar from the group. As Gonchar explained in a press conference at the Ukraine Crisis Media Center in June 2014, "the performance of the management and soldiers of the battalion AZOV should be [a] [concern] [to] the senior management of the Ministry of the Interior, because in fact they commit unlawful acts against their former colleagues."[9] Overall, as Khazin noted, "in May 2014, we saw very clearly for ourselves that the entire institutions: army, militia, intelligence, and internal troops – they were not ready for this war. They were, to put it mildly, in a bad state, with no way for them to fix it on their own. […] After the first battles in the east we realized that it was impossible to fight in such conditions. And we began to provide the army with clothes, shoes, walkie-talkies, summer armor, various devices such as sights and thermal imagers. And after some of us

---

[3] Eleonora Burdina, "Підполковник запасу ЗСУ Ярослав Гончар: «У Збройних силах кудись витрачаються мільярди гривень, а ІТ-продуктів не було і нема," *Dou*, June 10, 2021, https://dou.ua/lenta/interviews/about-it-problems-in-armed-forces/ or https://archive.ph/3m4vc

[4] Дата публікації, "АЕРОРОЗВІДКА ГОТОВА ВИГОТОВЛЯТИ І УКРАЇНСЬКІ "БАЙРАКТАРИ", АБИ ЛИШЕ НЕ СТРИМУВАЛИ КОРУПЦІЯ І ЗАСТАРІЛІ ПРОЦЕДУРИ," *TSN*, July 15, 2022, https://tsn.ua/ato/aerorozvidka-gotova-vigotovlyati-i-ukrayinski-bayraktari-abi-lishe-ne-strimuvali-korupciya-i-zastarili-proceduri-2111452.html or https://archive.ph/Kirem

[5] Богдана Костюк, "Україна-Ізраїль: від Жидівського куреня УГА і загонів «Хагани» – до Єврейської чоти УДА," *Radiosvoboda*, May 5, 2018, https://www.radiosvoboda.org/a/29208755.html or https://archive.ph/TY7oX

[6] Богдана Костюк, "«Автомайдан дискредитували, нас штрафували, брали під арешт і виносили неправосудні рішення, а машини палили» – Гончар," *Radiosvoboda*, November 26, 2017, https://www.radiosvoboda.org/a/28875554.html or https://archive.ph/QQ8mS

[7] Дарія ГОРСЬКА, "Командир еврейской сотни Майдана теперь спасает бойцов в зоне АТО," Fakty, December 9, 2014, https://fakty.ua/192310-komandir-evrejskoj-sotni-majdana-teper-spasaet-bojcov-v-zone-ato or https://archive.ph/hcVgx

[8] Unian, "Операция по освобождению здания милиции Мариуполя провалилась из-за несогласованности действий," *Unian*, December 5, 2014, https://www.unian.net/politics/917062-operatsiya-po-osvobojdeniyu-zdaniya-militsii-mariupolya-provalilas-iz-za-nesoglasovannosti-deystviy.html or https://archive.ph/WrIzG; Pieter van Huis, "A Reconstruction of Clashes in Mariupol, Ukraine, 9 May 2014," *Bellingcat*, January 28, 2015, https://www.bellingcat.com/news/uk-and-europe/2015/01/28/a-reconstruction-of-clashes-in-mariupol-ukraine-9-may-2014/ or https://archive.ph/alZLu

[9] UCMC Press Center, Оригінал статті - на сайті Українського кризового медіа-центру," *uacrisis*, June 6, 2014, https://uacrisis.org/en/3809-yaroslav-gonchar or https://archive.ph/nEB3s

joined the reconnaissance platoon of the 72nd [mechanized] brigade, we began to think about how to help them."[10]

Aerorozvidka's initial efforts were focused on creating, modernizing, and deploying commercial drones for the purpose of enhancing situational awareness and reconnaissance capabilities on the eastern front. Khazin pitched the drone idea and subsequently reached out to someone he met at the Maidan who used a DJI-Phantom drone to record panoramic videos. Khazin also travelled to Israel to meet with government officials there but was not successful in eliciting any assistance from them.

At the time, the Ukrainian Armed Forces had no drones in their arsenal, and as such also no experience of using them during an active shooting war. Aerorozvidka understood what the armed forces needed, and they had the skills and personal network to potentially fill that capability void. In many ways, Aerorozvidka's initial engineering efforts had more in common with Mad Max and MacGyver, as specific technical skills had to be identified, engineering solutions improvised, and replacement parts traded or tinkered together.

In June 2014, the group tested its first heavily modified DJI-Phantom drone named Fantik (Фантик), which Volodymyr Kochetkov-Sukach took to the Aidar Battalion in the Luhansk Oblast for a two-week test run.[11] Yaroslav Gonchar, in conjunction with several people from the "Krok" computer academy, took up the task of continuously modernizing Fantik. The team also began to actively search for talent on Facebook to join Aerorozvidka. As Khazin notes, "some of them were from our unit, from 'Azov,' we found some through Facebook, posting information and later created a closed group. We interviewed candidates 3-4 days a week and found another 20 extraordinary personalities. So, I thank Mr. Zuckerberg for the fact that we now know how to make a powerful sub-section thanks to Facebook. Social networks are also weapons."[12]

With the successful completion of Fantik's test-run, Aerorozvidka was officially founded on July 15, 2014. Its initial financial backing came primarily from civilian non-government groups and several individual patrons who made large donations in support of the cause.[13]

Figure 1-2: The first team of Aerorozvidka at the Yavoriv training ground in November 2014
Top left to right: Yury Grachov, X, Nathan Khazin, Oleksandr Kvyatkovskyi, X, Yaroslav Gonchar, Volodymyr Kochetkov-Sukach.
Bottom left to right: X, X

Source: (left) Наталка Позняк-Хоменко, "Волонтери: сила небайдужих," Український інститут національної пам'ят, Dec. 2020, p. 269;
(right) Aerorozvidka, "Аеророзвідці сьогодні 9 років," Telegram, July 15, 2023

[10] Наталка Позняк-Хоменко, "Волонтери: сила небайдужих," 2020, Український інститут національної пам'яті, https://uinp.gov.ua/elektronni-vydannya/volontery-syla-nebayduzhyh/zavantazhyty/volontery-syla-nebayduzhyh, p. 266 or https://web.archive.org/web/20230903184833/http://uinp.gov.ua/elektronni-vydannya/volontery-syla-nebayduzhyh/zavantazhyty/volontery-syla-nebayduzhyh, p. 266

[11] In September 2014, Amnesty International wrote a brief on the Aidar battalion titled: "Ukraine: Abuses and war crimes by the Aidar Volunteer Battalion in the north Luhansk region," see: Amnesty Interantional Brief, "Ukraine: Abuses and war crimes by the Aidar Volunteer Battalion in the north Luhansk region," September 2014, https://www.amnesty.org/en/documents/eur50/040/2014/en/

[12] Наталка Позняк-Хоменко, "Волонтери: сила небайдужих," 2020, Український інститут національної пам'яті, https://uinp.gov.ua/elektronni-vydannya/volontery-syla-nebayduzhyh/zavantazhyty/volontery-syla-nebayduzhyh, p. 268 or https://web.archive.org/web/20230903184833/http://uinp.gov.ua/elektronni-vydannya/volontery-syla-nebayduzhyh/zavantazhyty/volontery-syla-nebayduzhyh, p. 268

[13] Аеророзвідка, "Аеророзвідці сьогодні 9 років," *Telegram*, July 15, 2023, https://t.me/aerorozvidka/1234 or https://archive.ph/eEkS0; Eleonora Burdina, "Підполковник запасу ЗСУ Ярослав Гончар: «У Збройних силах кудись витрачаються мільярди гривень, а IT-продуктів не було і нема," *Dou*, June 10, 2021, https://dou.ua/lenta/interviews/about-it-problems-in-armed-forces/ or https://archive.ph/3m4vc

By the end of autumn 2014, Aerorozvidka had stood up an assortment of 12 multi-rotor drones. To test their equipment and to and exercise with the Ukrainian Armed Forces, Aerorozvidka deployed to the Yavoriv training ground (Яворівський полігон) in western Ukraine. Yavoriv is probably most well-known to Western observers for being the training base of the Ukrainian Foreign Legion, which was hit by a Russian air strike on March 13, 2022, that killed an estimated 35 to 180 personnel.[14] Tragically, Aerorozvidka's Yury Grachov – who was responsible for developing the drone's ammunitions – died in November 2014 during an accident at Yavoriv.[15]

In January 2015 – close to the end of the second battle for the Donetsk Airport – Aerorozvidka deployed its drone fleet to provide aerial reconnaissance on the front lines. As Gonchar explains it, "the first week's work changed the balance of power in this area: our guys knocked out several mortars and took the initiative. It was also the first time we faced the use of electronic warfare by the Russian army. We were completely unprepared for this. Add to that the fierce shelling - something was constantly falling on our heads. Thus, we lost some of our equipment. Two vehicles were damaged by Grad rockets, and several drones were blown apart. We did not even understand what was happening, and at first we blamed the developers who created the equipment."[16] Gonchar goes on to state that "the most fierce fighting was going on when the airport fell. It was hell there, our people were coming out, we were looking for them under the ruins: captures, exchanges... The demand for information was fierce. We saw that the five battalions that held the [Donetzk Airport] were up for grabs. So we did not sleep, we were constantly charging batteries and flying. We flew as much as we could. So when we lost this ability, it was terrible."[17]

The defense of the Donetzk Airport is deeply engrained in Ukraine's national consciousness. It was then and there that the myth of Ukraine's "cyborgs" – as Russian separatists called the persistent airport defenders – was born.[18] While open source is unclear when Aerorozvidka gained its own legendary status within the Ukrainian Armed Forces, it seems likely that it also emerged during the defense of the Donetsk Airport. On March 15, 2015, Volodymir Kochetkov-Sukach was killed by a trip-wire explosion in Krasnohorivka, on the outskirts of Donetsk.[19]

With the destruction of Aerorozvidka's entire drone fleet, the team eventually came up with the idea of providing aerial reconnaissance via stationary cameras. Within a week, they got their hands on multiple high-definition digital cameras which were organized by Oleksiy Mochanov – a former race driver and motor sport journalist – and Yuri Biryukov, then the advisor to President Poroshenko and assistant to then Defense Minister Stepan Poltorak.[20] The team also struck a deal with the Ukrainian telecommunications operator Datagroup, which provided them with eight satellite terminals and several months-long free subscriptions.[21] Aerorozvidka then proceeded to deploy the cameras in the field. As Gonchar explains it, "Donbas is a very industrialized area, there are many mines, towers, ... So, you can install the camera at a height of 20, 30, 40, 50 meters. The cameras operate around the clock and provide an overview of several kilometers. And it turned out an even more powerful tool for surveillance, targeting, and situational awareness."[22]

Aerorozvidka's overall approach to problem solving was non-hierarchical, functionally agile, technologically specialized, and goal oriented – which was entirely different from the bureaucratic 'I need written orders to do anything' paradigm the Ukrainian Armed Forces were still operating under. The Armed Forces eventually realized that they themselves did not have the in-house expertise to repair and maintain the stationary cameras in the field. And as a result, the military ended up delegating these maintenance tasks to Aerorozvidka and provided them with a budget to cover their activities.

Sometime in 2015, Aerorozvidka was eventually incorporated into the Ukrainian Armed Forces as military unit A2724 on the behest of Viktor Muzhenko, the then Chief

---

[14] Hugo Bachega, "Ukraine war: 'Sky turned red' as missiles hit Lviv military base," *BBC*, March 13, 2022, https://www.bbc.com/news/world-europe-60728208

[15] Аеророзвідка, "#Support_AERORozvidka Цей рейд присвячується нашому побратиму Юрію Грачову (Ірокезу). Він починав розробку боєприпасів, якими зараз нищать," *Facebook*, March 18, 2022, https://www.facebook.com/aerorozvidka/videos/350839936800484/

[16] Eleonora Burdina, "Підполковник запасу ЗСУ Ярослав Гончар: «У Збройних силах кудись витрачаються мільярди гривень, а IT-продуктів не було і нема," *Dou*, June 10, 2021, https://dou.ua/lenta/interviews/about-it-problems-in-armed-forces/ or https://archive.ph/3m4vc

[17] Ibid.

[18] Vitaly Shevchenko, "Ukraine conflict: The 'cyborg' defenders of Donetsk airport," *BBC*, October 31, 2014, https://www.bbc.com/news/world-europe-29793696

[19] Informnapalm, "They Killed Chewbacca," March 16, 2015, https://informnapalm.org/en/they-killed-chewbacca/

[20] Blpa.in.ua, "ПРО АЕРОРОЗВІДКУ," November 27, 2017, https://web.archive.org/web/20171127070426/http://bpla.in.ua/history.html

[21] Eleonora Burdina, "Підполковник запасу ЗСУ Ярослав Гончар: «У Збройних силах кудись витрачаються мільярди гривень, а IT-продуктів не було і нема," *Dou*, June 10, 2021, https://dou.ua/lenta/interviews/about-it-problems-in-armed-forces/ or https://archive.ph/3m4vc; https://www.data-group.ua/en/pro-kompaniyu

[22] Eleonora Burdina, "Підполковник запасу ЗСУ Ярослав Гончар: «У Збройних силах кудись витрачаються мільярди гривень, а IT-продуктів не було і нема," *Dou*, June 10, 2021, https://dou.ua/lenta/interviews/about-it-problems-in-armed-forces/ or https://archive.ph/3m4vc

of the General Staff of the Armed Forces, and Andriy Taranov, the then Deputy Head of – what is now known as – the Office of the President of Ukraine.[23]

Figure 3: Unit A2724's badge

As Nathan Khazin explained to news outlet Novinarnia in 2021, "the miracles we did, you can't even understand! We needed IT specialists, which were not available in the Armed Forces. And this was during the 4th and 5th wave of mobilization. I visited companies such as Intel and IBM Ukraine and asked people, 'have you received the [mobilization] summons yet?' Some received it. 'Then I have very good news for you: you will not go to dig trenches.' I literally removed one mobilized person from his car – the person was already on his way to dig trenches, but instead he joined us. Thanks to the mobilization efforts, we build up a team."[24]
Gonchar additionally contextualized that, "when we created the military unit, civil society helped us a lot, including IT professionals. Software companies began to visit the unit: Army SOS, Kropyva, SUVA, etc. It so happened that a unit had up to a dozen different software programs covering certain tasks. And since the IT and engineering community gathered in the A2724 military unit […], among other things, they had to integrate all the applications that were sent to the units."[25]

1.1 Army SOS & Kropyva (Кропива)

Army SOS was founded in March 2014 as a volunteer organization to provide modern equipment directly to units in the Armed Forces of Ukraine. The team grew from initially four to currently 19 members, which specifically focus on (a) the continuous development and deployment of Kropyva, and (b) the purchase of unmanned aerial vehicles. The group's activities are sustained via donations.

Kropyva (Engl. transl.: Nettle) is a proprietary software product that is specifically designed for military mission planning, calculating firing solutions, and providing quick and easy aerial orientation. It allows for data exchange with other users – including short messages and sharing positional coordinates – via anything from short-wave radios to satellite terminals. While GPS is mandatory, Kropyva "works completely offline and does not require access to the Internet."[26] Reportedly, its offline map function saved the lives of individual Ukrainian soldiers and entire units that lost their orientation on the vast battlefield. A technical support team is continuously improving the software and is adding new features. Military units can directly order Kropyva for free pre-installed on 20-25cm small tablets from the Army SOS website.[27] It is unknown how many devices Army SOS has shipped out over the course of the war.

According to Armyinform.com.ua, the origins of Kropyva go back to 2018 when developers from the Logika design bureau (Логіка) – which is part of the League of Defense Enterprises of Ukraine (Ліга оборонних підприємств України) – provided Army SOS with the Kropyva source code and a license to freely distribute the software to the Ukrainian Armed Forces.[28] With the Russian invasion on February 24, 2022, the dissemination of Kropyva subsequently skyrocketed. Speaking to Forbes in July 2022, Army SOS co-founder Alexey Savchenko stated that Kropyva is being used by 90-95% of Ukrainian artillery officers.

In terms of Kropyva's technical capabilities, Kravets et al. published a study in 2021 that looked at five Ukrainian geolocation systems in their normal hardware configurations, to investigate the devices speed and accuracy for determining correct GPS location coordinates. The systems included: Kropyva, MilChat, ArtOS (Артос), Ukrop (Укроп), and Bazalt M (Базальт М). According to the study's authors – who are all members of the Department for Artillery Reconnaissance Complexes and Devices at

[23] Ibid.

[24] Олена Максименко, "Армія майбутнього, що лишилася в минулому. Спогади творця розформованої "Аеророзвідки," Novynarnia, April 17, 2021, https://novynarnia.com/2021/04/17/khazin/

[25] Eleonora Burdina, "Підполковник запасу ЗСУ Ярослав Гончар: «У Збройних силах кудись витрачаються мільярди гривень, а ІТ-продуктів не було і нема," *Dou*, June 10, 2021, https://dou.ua/lenta/interviews/about-it-problems-in-armed-forces/ or https://archive.ph/3m4vc

[26] Army SOS, "Вимоги для планшетів," n.d., https://docs.google.com/document/d/1DsvHmV7t5zExS1T-Ndng9nChAMOh4T21XIg91nLCR44/edit or https://archive.ph/OIIZ6; Note: It is unclear whether Kropyva also works with other GNSS services, such as Galileo.

[27] Army SOS, "Кропива," n.d., https://armysos.com.ua/uk/kropyva/ or https://web.archive.org/web/20240522142645/https://armysos.com.ua/uk/kropyva/; Army SOS, "форма замовлення планшетів," n.d., https://forms.gle/AqcSDnL3SUUrnCUx6

[28] Микола Федорків, "Для чого «Кропива» потрібна військовим," *Armyinform*, July 6, 2020, https://armyinform.com.ua/2020/07/06/dlya-chogo-kropyva-potribna-vijskovym/ or https://web.archive.org/web/20240522142734/https://armyinform.com.ua/2020/07/06/dlya-chogo-kropyva-potribna-vijskovym/

Ukraine's Hetman Petro Sahaidachny National Army Academy – the investigation was necessary because ,"although Kropyva, Ukrop, and ArtOS are approved for use in the Armed Forces of Ukraine, and Basalt-M is in service with the troops or is actively used, in particular in the Joint Forces Operation (JFO) area, there has been no comparison of the accuracy of coordinate determination and no recommendations for its use. There are no scientific papers on the accuracy of coordinate determination by instruments in relation to the catalog of coordinates of geodetic points and the list of coordinates of special geodetic boundary points in Ukraine."[29]

Kravet's et al. conducted three types of tests: (1) Reading the GPS coordinate immediately after the devices have been switched on (i.e. a cold start), (2) reading them after 15 minutes, and (3) reading them after 30 minutes (i.e., recalibration). The conclusion of the tests was that a cold start resulted in MilChat showing a location with a positioning error of 3 meters, Basalt-M of 9 meters, Kropyva of 15 meters, ArtOS of 14 meters, and Ukrop of 28 meters. While MilChat had the smallest error, Kropyva provided coordinates in half the time than the other 4 devices. After 15 minutes, MilChat still had an error of 3 meters, Basalt-M recalibrated to only 1 meter, Kropyva to 1.5 meters, Atos to 3 meters, and Ukrop to 22 meters. After 30 minutes, MilChat had an error of 2.5 meters, Basalt-M stayed at 1 meter, Kropyva had only an accuracy error of 0.75 meters, Atos stayed at 3 meters, and Ukrop recalibrated to 20 meters.

The findings of Kravets et al. suggest that Kropyva's hard- and software package is the most optimal battlefield solution. Meanwhile, MilChat might be most beneficial when operating in a highlight contested electronic warfare environment that only allows for cold starts and very tight signal reception windows.

Speaking to Forbes Ukraine on April 24, 2023, Ruslan Prylypko, head of Aerorozvidka NGO's IT department, explained that "the developers of Delta recently informed users about a new feature – importing and exporting settings from Kropyva to Delta. Now you can share the situation in Kropyva with Delta users. Or you can add information from Delta to your situational awareness that is missing in Kropyva itself."[30]

Figure 4-7: Army SOS Gallery: Kropyva

Source: ArmySOS, "Фотозвіти," n.d., https://armysos.com.ua/uk/gallery-ua/

The Russian Ministry of Defense was not sitting on its hands while the Ukrainians were innovating. In September 2023, the Ukrainian state-coordinated hacking group Kyber Sprotyv (Engl. transl.: Cyber Resistance) breached the email account of Lt. Col. Yuri Vishnyakov, who is an employee within the Organizational Branch of the Russian National Guard's Special Forces (Організаційного відділення Сил Спеціального Призначення Росгвардії). Among the exfiltrated files was a Power Point presentation of a Russian prototype software application named Repei (Репей), created by Russian electronic warfare manufacturer Sozvezdie (Созвездие).[31] On slide three, the presentation explicitly mentions Kropyva as the enemy's counterpart system. The National Resistance Center – which was created by the Ukrainian Special Operations Forces – published screenshots of the slides on its website and noted that, "ideology, functional architecture, and even the interface [have been copied from] the Ukrainian automated management system [Kropyva]

[29] Т. КРАВЕЦЬ et al., "АНАЛІЗ СЕРЕДНЬОКВАДРАТИЧНОГО ВІДХИЛЕННЯ АПАРАТУРИ "КРОПИВА", "УКРОП", "ARTOS" ТА "БАЗАЛЬТ-М" ВІДНОСНО КАТАЛОГУ КООРДИНАТ ГЕОДЕЗИЧНИХ ПУНКТІВ," Сучасні досягнення геодезичної науки та виробництва, випуск II (42), 2021, https://web.archive.org/web/20240216135149/http://zgt.com.ua/wp-content/uploads/2021/09/3.pdf, p. 18

[30] Таїса Мельник, "«Цифровізація в армії ще не починалася». Керівник ІТ-напряму «Аеророзвідки» про експорт Delta, $50 млн на фронтову кібербезпеку та ленд-ліз для інновацій," *Forbes Ukraine*, April 24, 2023, https://forbes.ua/innovations/tsifrovizatsiya-v-armii-shche-ne-pochinalasya-kerivnik-it-napryamku-aerorozvidki-pro-eksport-delta-50-mln-na-frontovu-kiberbezpeku-ta-lendliz-dlya-innovatsiy-24042023-13182 or https://web.archive.org/web/20240522084007/https://forbes.ua/innovations/tsifrovizatsiya-v-armii-shche-ne-pochinalasya-kerivnik-it-napryamku-aerorozvidki-pro-eksport-delta-50-mln-na-frontovu-kiberbezpeku-ta-lendliz-dlya-innovatsiy-24042023-13182

[31] Kyber Sprotyv, "Чим займається кожен представник російського репресивного апарату у званні від майора і вище?" Telegram, September 26, 2023, https://t.me/cyberResistanceUA/292 or https://archive.ph/xbxQm; For more context on Kyber Sprotyv see: Stefan Soesanto & Wiktoria Gajos, "Kyber Sprotyv: Ukraine's Spec Ops in Cyberspace?" Lawfare, April 9, 2024, https://www.lawfaremedia.org/article/kyber-sprotyv-ukraine-s-spec-ops-in-cyberspace

completely. There are also offline maps, and switching between [map] layers, and calculations of visibility zones and fire based on 3D models of the relief."[32]

In May 2024, Ukraine's State Service of Special Communications and Information Protection (SSSCIP) noted in its H2 2023 APT Activity Report #3 that "in one of the cases of the second half of 2023, the Russian military intelligence agency disguised the open-source code of the spy program for Android - SPYNOTE (SpyMax) - as the Nettle [Kropyva] system installer. Unfortunately, we have to state that the main delivery channel outside of Google Play, which is blocked by the SPZ, remains social engineering during communication via Signal and Telegram."[33]

* * * *

Aerorozvidka's integration into the military's hierarchy came with certain trade-offs. On the one hand, it created new obstacles. For example, funds to buy equipment or to pay companies for their expertise became so bureaucratic that it took the Ukrainian Ministry of Defense months to process outgoing payments. On the other hand, Aerorozvidka gained invaluable insights into the specific technical and informational needs across the various levels of the armed forces. Speaking about the forward deployed HD cameras, Gonchar noted that, "a forward observer looks at the monitor, several pictures are displayed in front of him, he understands where the cameras are and so he navigates. But when the [military] headquarters started sending requests to see the same content, it became clear that we needed to build a network. Because people in the headquarters are not on the front line, they have other jobs, they do not understand what, whe[n], where, what are the coordinates. There was a need to mark objects on video. We contacted the volunteer association ComBat Vision, headed by Yevhen [Eugene] Maksymenko, and set this task as part of the development (they were simultaneously developing a tactical client for a soldier). And they implemented this functionality."[34]

1.2 ComBat Vision

The origins of ComBat Vision (комбат) go back to 2012, when Eugene Maksymenko – then an application developer at Ukraine's largest IT project distributor Megatrade – created an Android-based location sharing application for his friends.[35] As Maksymenko explained to dou.ua, "back in 2012, I was raising young people in a military-patriotic spirit and was one of the founders of the ARMS-Project club. Our team organized hiking trips to the wilderness with elements of certain military tasks (reconnaissance, search for cargo or paratroopers, rescue of the wounded, etc.) When the team grew to several hundred people, the problem arose of understanding where a large number of groups were, what they were doing, and what difficulties they were having. Then we came up with the idea to create a simplified analog of the military's situational awareness system (C4I), which was gaining momentum in various leading armies around the world."[36]

In its most recent 4.0 version, ComBat Vision is a distributed geospatial information platform. It is distributed in the sense that the system does not have a central node anymore. Instead, each device stores part of the information and can delegate access to other users using end-to-end encryption. The logic behind this segmented setup is that a scout does not need to know the locations of all the troops on the battlefield. Instead, he is given access to see and enter data for a certain geographic area. To exchange information and ensure interoperability, ComBat is built around the NATO Standard Agreement (STANAG) 4677 Joint Dismounted Soldier System (JDSS) protocol. As the ComBat website notes, this was done to ensure that separate units can operate in an environment of unstable and slow communications, as the system "works even with [high frequency] radio communication at a speed of 1 Kbps."[37] Similarly, the STANG implementation also allows for NATO integration and potential future sales to NATO member states.

---

[32] National Resistance Center, "Hackers from 'Cyber resistance' gained access to technical documentation of the Russian counterfeit "Kropiva," September 26, 2023, https://sprotyv.mod.gov.ua/en/hackers-from-cyber-resistance-gained-access-to-technical-documentation-of-the-russian-counterfeit-kropiva/ or https://archive.ph/DkkqM

[33] SSSCIP, "Russian Cyber Operations- APT Activity Report 3 H2 2023," May 3, 2024, https://docs.google.com/viewer?url=https://cip.gov.ua/services/cm/api/attachment/download?id=64622&embedded=true&a=bi or https://archive.ph/jxKHX, p. 21

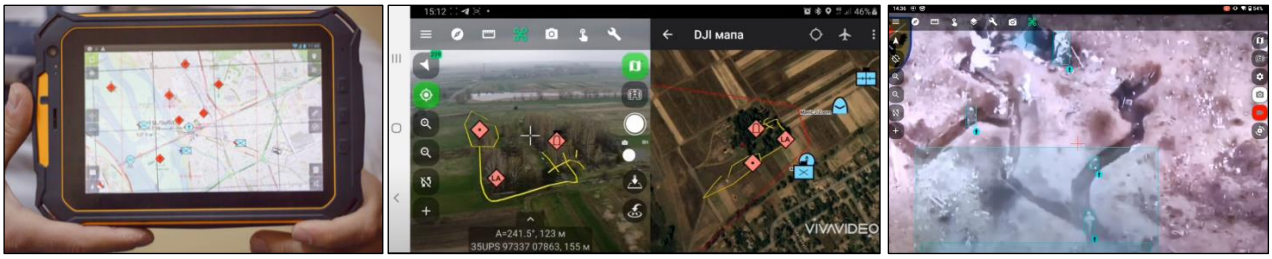
[34] Eleonora Burdina, "Підполковник запасу ЗСУ Ярослав Гончар: «У Збройних силах кудись витрачаються мільярди гривень, а IT-продуктів не було і нема," *Dou*, June 10, 2021, https://dou.ua/lenta/interviews/about-it-problems-in-armed-forces/ or https://archive.ph/3m4vc

[35] Українська правда, "Інновації для армії. Навігація для військових 'КомБат'," May 12, 2015, https://life.pravda.com.ua/society/2015/05/12/193822/ or https://web.archive.org/web/20240521143832/https://life.pravda.com.ua/society/2015/05/12/193822/

[36] Eugene Maksymenko, "C4 Vision system — розподілена система обміну інформацією для військових від S.T.A.R Vision," *Dou*, July 23, 2019, https://dou.ua/lenta/articles/dou-projector-c4istar/ or https://web.archive.org/web/20240521144035/https://dou.ua/lenta/articles/dou-projector-c4istar/

[37] Combat.Vision, "Combat Vision 4.0, Battlefield Reconnaisance and Coordination System," n.d., https://combat.vision/ or https://web.archive.org/web/20230516114909/https://combat.vision/

Figure 8-10: ComBat Vision platform, force coordination, and target identification



Source: (left) Українська правда, "Інновації для армії. Навігація для військових 'КомБат'," May 12, 2015;
(center + right) ComBat Vision Youtube channel

Combat Vision functions with any IP compatible connection, including, WiFi, 3G/LTE, and both Starlink terminals and ViaSat's Tooway modems.[38] According to Combat Vision's website, the software now even includes augmented reality, a 3D map that works offline, a messaging system, movable line of sight calculators, and it can pull data from drones, stationary cameras, and other sources for relaying targeting information.[39] Because of its compact design and data driven input, Maksymenko notes that "this system is not intended for shooting and marking something on the go. No one clicks in combat. The system is needed to reach the goal, indicate the situation on the map, work it out and conduct an analysis."[40]

According to Maksymenko, the initial period to develop Combat Vision took a mere six months, with another six months spent on finding an investor to stabilize the project's funding. As he put it, "we are volunteers in that we made this program for 2-3 times less money than if we were working on a commercial project. It's impossible to sit and develop something for six months without a salary, but now we are all losing money. We could have earned much more."[41]

The funding for developing ComBat Vision, as well as for buying the computers, laptops, and tablets to deploy the software on was primarily provided through David Arakhamia's People's Project website. Outside of Ukraine, David Arakhamia is probably most well-known for being the leader of Ukraine's Servant of the People political party, and for heading the Ukrainian peace delegation to Istanbul, Turkey, in March 2022.[42]

Arakhamia created the People's Project back in the Spring of 2014 amidst the annexation of Crimea and the war in Donbas.[43] The People's Project is a non-commercial non-profit platform that is run by volunteers who coordinate multiple online crowdfunding efforts. This includes for example, raising 23.000 USD to purchase thermal imagers for the Ukrainian Armed Forces, 5.500 USD for the chemotherapy of a combat pilot named Ivan, and collecting 20.000 USD to purchase necessary equipment for the Burn Unit at the Cherkasy First City Hospital.[44] The cost for Combat Vision's deployment are roughly 500 USD for a tablet, 2.500 USD for a rugged laptop, and 800 USD for a walkie talkie.[45]

Speaking to Swiss magazine L'Illustré in 2022, Maksymento explained that back in 2015 he offered Combat Vision to the Ukrainian high command, but "once the hot phase of the Donbass war was over, [they] lost interest in it. […] Our army could be fully automated today. But the level of attention of our generals is apparently dependent on the distance between Kyiv and the Orcs [the Russians]."[46] Instead, in April 2015, Combat Vision was tested by Ukraine's Special Operations Forces and merely touted for broader military adoption.[47] As Makysmenko noted to

[38] Ibid.

[39] Ibid.

[40] Українська правда, "Інновації для армії. Навігація для військових 'КомБат'," May 12, 2015, https://life.pravda.com.ua/society/2015/05/12/193822/ or https://web.archive.org/web/20240521143832/https://life.pravda.com.ua/society/2015/05/12/193822/

[41] Ibid.

[42] Ruth Michaelson, "'The world is waiting for good news': Russia-Ukraine peace talks press on in Turkey," The Guardian, March 29, 2022, https://www.theguardian.com/world/2022/mar/29/the-world-is-waiting-for-good-news-russia-ukraine-peace-talks-press-on-in-turkey

[43] People's Project, "Who we are," n.d. https://www.peoplesproject.com/en/about/ or https://web.archive.org/web/20240521144428/https://www.peoplesproject.com/en/about/

[44] People's Project, "Thermal imagers for the army," n.d., https://www.peoplesproject.com/en/thermal-imagers-for-the-army/ or https://web.archive.org/web/20240521144636/https://www.peoplesproject.com/en/thermal-imagers-for-the-army/; People's Project, "Saving Ivan. Stage IV," n.d., https://www.peoplesproject.com/en/vryatuvati-ivana/ or https://web.archive.org/web/20240521144803/https://www.peoplesproject.com/en/vryatuvati-ivana/; People's Project, "Operation Burn," n.d., https://www.peoplesproject.com/en/operaciya-opik/ or https://web.archive.org/web/20240521144757/https://www.peoplesproject.com/en/operaciya-opik/

[45] Александр Мельник, "Украинский спецназ получил систему электронной координации «КомБат», разработанную волонтёрами," *imena.ua*, May 13, 2015, https://www.imena.ua/blog/ua-combat/ or https://web.archive.org/web/20240522083016/https://www.imena.ua/blog/ua-combat/

[46] Hubert Migeot, "L'innovation technologique au service de la résistance ukrainienne," *L'illustre*, June 27, 2022, https://www.illustre.ch/magazine/linnovation-technologique-au-service-de-la-resistance-ukrainienne-387798

[47] Александр Мельник, "Украинский спецназ получил систему электронной координации «КомБат», разработанную

defence-ua, "in 2015-2018, the effectiveness of […] ComBat Vision was already confirmed in real conditions by units of the Special Operations Forces, a number of which adopted our product. Why them? First, we decided that our development will be more important specifically for SSO [Special Operations Forces] groups or, for example, DSHV [Ukrainian Air Assault Forces], which conduct raids on the enemy's rear. Second, only SSOs had the necessary equipment to integrate our system."[48] Maksymenko also provided a simpler explanation to pravda.com.ua, saying "[regular soldiers] get scared, even when the screen on the tablet simply goes out. That's why we are primarily determined to start with special units, where more or less specialists are gathered."[49]

With the start of the Russian invasion on February 24, 2022, Combat Vision 3.0 was eventually deployed to 83 military units of various sizes. Maksymenko notes that, "at that time, we already had the third generation of our system, but with the beginning of the war, we realized that continuing to implement 10-year-old technology is not a very promising story, and we took a one-year timeout to develop a new, fourth-generation system with new capabilities, in the context of the integration of NATO standards in the Armed Forces, rethinking the entire experience of applying ComBat Vision."[50]
As of this writing, it is unknown whether Combat Vision feeds or will feed information directly into Delta.

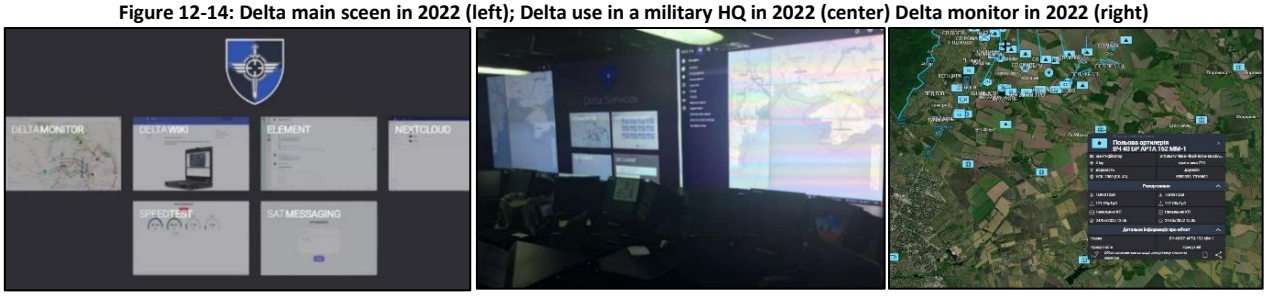
2 Delta (Дельта)

In the spring of 2016, Aerorozvidka presented a situational awareness platform prototype – now known as Delta – to the Ministry of Defense and then President of Ukraine Petro Poroshenko. Delta is a software platform that aims to provide military commanders across all levels with the freedom to plan operations and combat missions in coordination with other units.

Figure 11: Delta logo

It allows for secure information exchange, the sharing of location data of enemy forces, and quick access to up-to-date information on sector or battlefield-wide developments. As of this writing, Delta is hosted on cloud servers in Ukraine and is accessible from anywhere in the world via its url: delta.mil.gov.ua. As the New York Times noted in 2022, "what NATO officials said was surprising about the Delta system was that the network was so broadly accessible to troops that it helped them make battlefield decisions even faster than some more modern militaries."[51] The Delta website is available in both Ukrainian and English. It is likely that several NATO member states have been granted access to the Delta platform.

Figure 12-14: Delta main sceen in 2022 (left); Delta use in a military HQ in 2022 (center) Delta monitor in 2022 (right)



Source: (left) JokerDPR, "Продолжаем унижать самоуверенных украинцев программой управления войсками DELTA," *Telegram*, Nov. 3, 2022; (center) Олена Максименко, "Армія майбутнього, що лишилася в минулому. Спогади творця розформованої "Аеророзвідки'," *Novyarnia*, April 17, 2021; (right) JokerDPR, ibid.

волонтёрами," *imena.ua*, May 13, 2015, https://www.imena.ua/blog/ua-combat/ or https://web.archive.org/web/20240522083016/https://www.imena.ua/blog/ua-combat/

[48] "Поле бою в realtime: на що здатна система управління тактичного рівня ComBat Vision від українського розробника,"*defence-ua.com*, July 21, 2023, https://defence-ua.com/people_and_company/pole_boju_v_realtime_na_scho_zdatna_sistema_upravlinnja_taktichnogo_rivnja_combat_vision_vid_ukrajinskogo_rozrobnika-12273.html or https://web.archive.org/web/20240522083244/https://defence-ua.com/people_and_company/pole_boju_v_realtime_na_scho_zdatna_sistema_upravlinnja_taktichnogo_rivnja_combat_vision_vid_ukrajinskogo_rozrobnika-12273.html

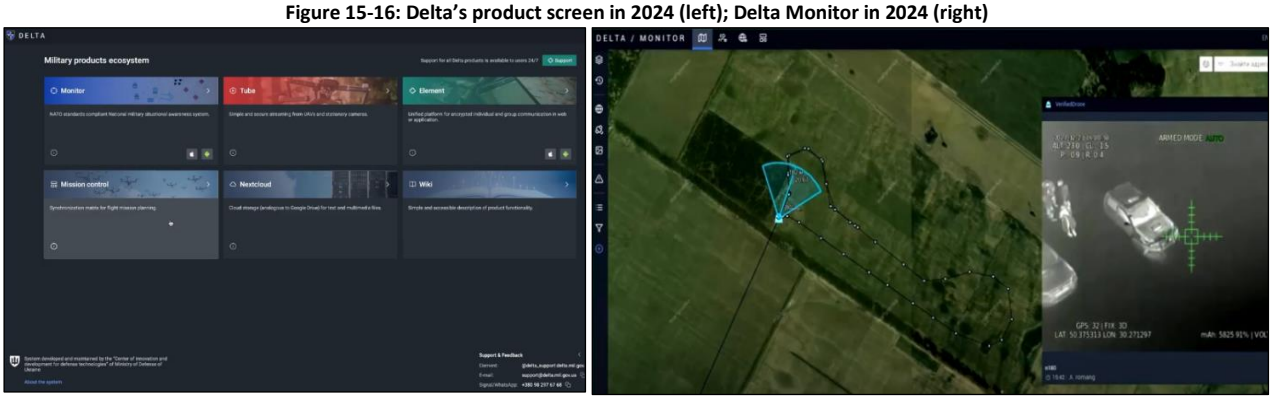
[49] Українська правда, "Інновації для армії. Навігація для військових 'КомБат'," May 12, 2015, https://life.pravda.com.ua/society/2015/05/12/193822/ or https://web.archive.org/web/20240521143832/https://life.pravda.com.ua/society/2015/05/12/193822/

[50] "Поле бою в realtime: на що здатна система управління тактичного рівня ComBat Vision від українського розробника,"*defence-ua.com*, July 21, 2023, https://defence-ua.com/people_and_company/pole_boju_v_realtime_na_scho_zdatna_sistema_upravlinnja_taktichnogo_rivnja_combat_vision_vid_ukrajinskogo_rozrobnika-12273.html or https://web.archive.org/web/20240522083244/https://defence-ua.com/people_and_company/pole_boju_v_realtime_na_scho_zdatna_sistema_upravlinnja_taktichnogo_rivnja_combat_vision_vid_ukrajinskogo_rozrobnika-12273.html

[51] Lara Jakes, "For Western Weapons, the Ukraine War Is a Beta Test," *New York Times*, November 15, 2022, https://www.nytimes.com/2022/11/15/world/europe/ukraine-weapons.html

As of this writing, the Delta platform consists of four key services: (1) Delta Monitor, (2) Element, (3) Delta Tube, and (4) Mission Control, and (5) Nextcloud. Delta Monitor is a multilayered digital map that allows for the tracking of enemy and defense forces, critical infrastructure (internet cables, gas lines etc.), and other tactical objects on the battlefield. The information displayed is constantly updated with new satellite imagery, radar and sensors in the field, such as GPS trackers, information received via the eEnemy and Stop Russian War Telegram chatbots, as well as other information received via third parties (i.e., NATO member states and others). Element is a secure messenger solution that enables coordination between units. Delta Tube allows for "a safe way to stream video from UAVs (copters, wings), stationary cameras, [and] any other video sources to any interested users and units in Delta."[52] Mission Control is a "synchronization matrix for flight mission planning." And Nextcloud is essentially cloud storage for documents and other media files like Google Drive. Delta's admin panel includes two additional tabs for User Management and Delta Intelligence. Delta Intelligence might be the place where data and pictures from mobile applications are stored.

Figure 15-16: Delta's product screen in 2024 (left); Delta Monitor in 2024 (right)



Source: NATO Allied Command Transformation, "Ukrainian MoD tests battlespace management system for NATO interoperability during CWIX 2024," Youtube, July 12, 2024, https://www.youtube.com/watch?v=TnPSDVDKhK8

2.1 NATO C4 Trust Fund

The initial development of Delta was a coordinated effort that in part was supported by the voluntary financial contributions and technical assistance from a handful of NATO member states. NATO's efforts in this area go back to the Wales Summit in 2014, when the alliance established a 1.8 million USD targeted trust fund to push Ukraine's communication, command and control, and computing systems (C4 for short) into the 21st century – away from Soviet-era centralized thinking.[53] As Gerard Elzinga, head of the Spectrum and C3 Infrastructure Branch at NATO HQ explained, "although it may not be a lot, it can be a game changer, with a little money and investing in the right projects, you can make a significant change to the capabilities that a nation has, and that has certainly proven its worth in Ukraine."[54]

NATO has since created several other dedicated trust funds in support of Ukraine, including the 'Cyber Defense Trust Fund' led by Romania, and the 'Logistics and Standardization Trust Fund' led by Czechia, Poland, and the Netherlands. The NATO-Ukraine C4 Trust Fund – as it is officially called – is led by Canada, Germany, and the UK. A 2018 brochure compiled by the East European Security Research Initiative Foundation with the support from the NATO Information and Documentation Centre in Ukraine, lists four projects under its umbrella with a combined budget of 2.75 million USD. Two of these projects have been – and still are – of relevance for the continuous development of Delta: The Situational Awareness Project and the Knowledge Sharing Project.
Delta essentially evolved out of the Situational Awareness Project, which is described in the 2018 brochure as "aim[ing] at assisting Ukrainian security and defence sector in enhancing overall situational awareness in accordance with the NATO standards."[55]

[52] Центр інновацій та розвитку оборонних технологій Міністерства оборони України, "Що таке DELTA?" Delta Wiki, n.d., https://delta.mil.gov.ua/wiki/info/#_2 or https://web.archive.org/web/20240110105843/https://delta.mil.gov.ua/wiki/info/#_2

[53] Kimberly Underwood, "NATO's Support of Ukraine's C4 Capabilities," *Signal*, December 7, 2023, https://www.afcea.org/signal-media/defense-operations/natos-support-ukraines-c4-capabilities or https://web.archive.org/web/20240522084136/https://www.afcea.org/signal-media/defense-operations/natos-support-ukraines-c4-capabilities

[54] Ibid.

[55] EESRI, "NATO's Support to Ukraine – Brief Guide," December 2018, https://eesri.org/wp-content/uploads/2018/12/NATO_Support_UA_leaflet2018_EESRI_ENG_web.pdf or https://web.archive.org/web/20240423091200/https://eesri.org/wp-content/uploads/2018/12/NATO_Support_UA_leaflet2018_EESRI_ENG_web.pdf

It is unknown when exactly, and how much financial and technical assistance military unit A2724 (Aerorozvidka) received via the NATO-Ukraine C4 Trust Fund for the development of Delta. Starting in 2016, most of Delta's funding might actually not have come via NATO but was donated by then Ukrainian President Poroshenko himself. Yuri Biryukov, then advisor to then President Poroshenko, alluded to this in a December 2016 Facebook post which highlighted the visit of Ukrainian Defense Minister Stepan Poltorak to Aerorozvidka, noting that "if only you knew who one of the largest 'donors' of this group is. Oh my goodness...."[56]

2.2 TIDE Hackathon

Since 2017, Delta has been part of the Knowledge Sharing Project which "aims at sharing NATO's C4 information, knowledge, and experience with Ukraine[,] as well as providing Ukraine with direct access to NATO and National Subject Matter Experts."[57] To a large degree the Knowledge Sharing Project has been facilitated by the Allied Command Transformation's (ACT) Interoperability Continuum, which consist of three event series: The Think-Tank for Information Decision and Execution (TIDE) Sprint, the TIDE Hackathons, and NATO's annual Coalition Warrior Interoperability eXploration, eXperimentation, eXamination, eXercise (CWIX). According to ACT, the purpose of the three events is "to ensure that our command and control capabilities can exchange operational information in the right format, to the right person at the right time so that NATO commanders and decision makers have the situational awareness needed to make good decisions, quickly!"[58]

The TIDE Sprint event takes place twice per year in different cities across NATO territory. At the 2024 TIDE Sprint in Dresden, Germany, more than 500 "operators, engineers, scientists, and technicians from government agencies, militaries, academia, and industry sectors" got together to utilize "a combination of presentations, brainstorming sessions, educational seminars, demonstrations, and testing to enhance NATO and National capabilities with a specific focus on interoperability."[59]
In October 2022 – eight months after the Russian invasion – Serhii Halchynskyi and Artem Martynenko from the Center for Innovation and Development of Defense Technologies, officially unveiled the Delta system at TIDE Sprint 2022 in Virginia Beach, USA.[60] Ukrainian Minister of Digital Transformation Mykhailo Fedorov spoke via recorded video message emphasizing that, "Delta is an amazing example of how Ukraine and NATO can cooperate, jointly develop and receive mutual benefits. […] But what's even more important, we are in the process of testing and introducing new standards for NATO."[61]

Figure 17: Delta unveiled at TIDE Spring 2022

Source: mil.in.ua, "Ukraine unveiled its own Delta situational awareness system," October 27, 2022.

The origins of the TIDE Sprint Hackathon go back to 2009, when a small group of attendees got together to launch the Enterprise Architecture (EA) track. In 2016, the first EA Hackathon was held in Krakow, Poland.[62] As ACT put it, "at this event, the participants will develop, produce and promote their solutions to the given challenges. They will work in teams; a selection board will validate the solutions and award the winner."[63] Following the success of two EA Hackathons, the event was rebranded into the TIDE Hackathon.

[56] Юрий Бирюков, "Волонтеры, беспилотники," *Facebook*, December 7, 2016, https://archive.ph/hzEOr

[57] EESRI, "NATO's Support to Ukraine – Brief Guide," December 2018, https://eesri.org/wp-content/uploads/2018/12/NATO_Support_UA_leaflet2018_EESRI_ENG_web.pdf or https://web.archive.org/web/20240423091200/https://eesri.org/wp-content/uploads/2018/12/NATO_Support_UA_leaflet2018_EESRI_ENG_web.pdf

[58] NATO ACT, "Coalition Warrior Interoperability Exercise," NATO's Strategic Warfare Development Command, n.d., https://www.act.nato.int/our-work/exercises/coalition-warrior-interoperability-exercise/ or https://web.archive.org/web/20240522091711/https://www.act.nato.int/our-work/exercises/coalition-warrior-interoperability-exercise/

[59] NATO ACT, "TIDE Sprint 2024: Advancing Interoperability," NATO's Strategic Warfare Development Command, n.d., https://www.act.nato.int/article/tide-sprint-2024-advancing-interoperability/ or https://archive.ph/aVirA

[60] Mil.in.ua, "Ukraine unveiled its own Delta situational awareness system," October 27, 2022, https://mil.in.ua/en/news/ukraine-unveiled-its-own-delta-situational-awareness-system/ or https://archive.ph/tDZaR

[61] We Are Ukraine, "Ukraine presented its situational awareness system at the NATO Tide Sprint event," November 13, 2022, https://www.weareukraine.info/ukraine-presented-its-situational-awareness-system-at-the-nato-tide-sprint-event/ or https://archive.ph/Fhs1P

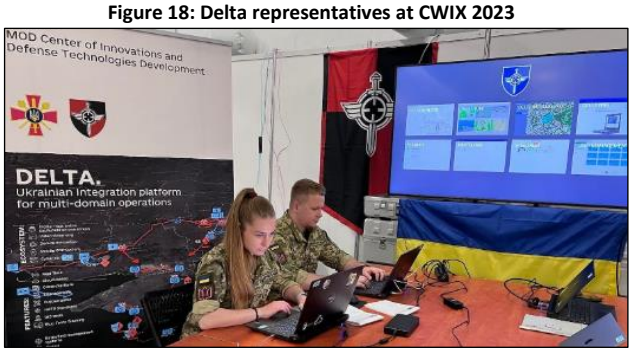
[62] ACT C2DS, "NATO Enterprise Architecture Hackathon," NATO ACT, March 16, 2016, http://www.act.nato.int/ea-hackathon or https://web.archive.org/web/20160512172802/http://www.act.nato.int/ea-hackathon

[63] ACT C2DS, "First-ever NATO Enterprise Architecture Hackathon," NATO ACT, February 22, 2026, https://www.act.nato.int/first-ever-nato-enterprise-hackathon or https://web.archive.org/web/20160507201645/https://www.act.nato.int/first-ever-nato-enterprise-hackathon

Nowadays, the event brings together "young, enthusiastic coders, engineers, architects, Information Technology experts and yes, hackers – to infuse energy into NATO's complex interoperability challenges."[64] The 2018 TIDE Hackathon handbook explains the objectives as following: To (1) "develop innovative architectural models, views, and methods for presented business cases," (2) "develop novel software/hardware based solutions for the 'low-hanging fruits' business cases," and (3) to "promote [NATO's] 'Interoperability by Design' principle and Enterprise Architecture (EA) discipline by sharing knowledge and increasing awareness among EA stakeholders."[65]
The Delta team won first place at the 2017 TIDE Hackathon in the Joint Challenge and Coding Challenge.[66] And in 2018 it won first place in the Modeling Challenge.[67] At the 2023 TIDE Hackathon, representatives from the Center for Innovation and Development of Defense Technologies briefed attendees about the latest Delta system developments.[68]

At this year's TIDE Hackathon in Amsterdam, two engineering teams (Valkyrie-1 and 2) from Ukraine's software development company SoftServe won the wargaming large language model (LLM) challenge and the pharmaceutical thesaurus challenge with their solutions.[69]

Figure 18: Delta representatives at CWIX 2023



Source: NATO in Ukraine "Представники Центру інновацій Міністерства оборони України успішно виступили на щорічних навчаннях НАТО – CWIX," Facebook, July 7, 2023.

NATO's annual Coalition Warrior Interoperability eXploration, eXperimentation, eXamination, eXercise (CWIX) is the alliance's largest interoperability event in which "alliance and partner nations make sure that their command and control capabilities de-risk interoperability as an essential first-step toward NATO missions." It also serves as "testbed for interoperability specifications that are hard-wired into experimental and near-fielded capabilities, ready for future NATO missions."[70] Since 2018, the Ukrainian Armed Forces – and with it the Delta team – have been participating in CWIX as full members.[71] In July 2023, representatives from the Center for Innovation and Development of Defense Technologies took part at CWIX in Bydgoszcz, Poland. On July 12, 2024, NATO's Strategic Warfare Development Command published an article on Delta at CWIX24. In it, Yelyzaveta Boiko, the Center's capability lead explains that "DELTA is an ecosystem of different military products. We actually call it 'Google for military' because after a single login, you have access to different modules in the system. Google helps to organize your workspace, DELTA helps to organize your 'war' space."[72]

According to NATO's Representation to Ukraine, "the [Delta] team had the opportunity to test 4 protocols for interaction with 15 other systems from 10 countries and NATO, and also participated in 12 of the 19 directions of CWIX. One of the key results is the successful testing of the Link 16 protocol, which will potentially allow Ukraine to integrate data from platforms and systems provided by donor states, such as F-16 aircraft."[73] Speaking to AFCEA's Signal magazine in December 2023, Gerard Elzinger added that Delta, "integrates with various NATO data links, including the Link-16 system and the GPS trackers that are part of the Iridium system. It combines various video feeds from drones, but also from mobile phones, for example. And with that, they can come up with a full common operational picture of the battlefield."[74] As of this writing, no F-16 aircrafts have been delivered to Ukraine.

---

[64] NATO ACT, "TIDE Hackathon Concludes in Amsterdam," NATO's Strategic Warfare Development Command, February 23, 2024, https://www.act.nato.int/article/tide-hackathon-concludes-amsterdam/ or https://archive.ph/xqDOR

[65] NATO, "2018 TIDE Hackathon Handbook," January 18, 2018, https://www.ucg.ac.me/skladiste/blog_1267/objava_20183/fajlovi/Hackathon%20Handbook.pdf, p. 7 or https://web.archive.org/web/20240423121321/https://www.ucg.ac.me/skladiste/blog_1267/objava_20183/fajlovi/Hackathon%20Handbook.pdf, p.7

[66] Aerorozvidka NGO, "Команда Центру інновацій та розвитку оборонних технологій Міністерства оборони взяла участь у найбільшій технічній конференції в Україні React+TS fwdays'23," *Linkedin*, October 2023, https://archive.ph/KSwDl

[67] National Security and Defense Council of Ukraine, "Ukrainian teams won prizes in NATO TIDE Hackathon 2023," February 2, 2023, https://www.rnbo.gov.ua/en/Diialnist/6142.html or https://archive.ph/okRTR

[68] Ibid.

[69] Softserve, "Softserve engineers win NATO TIDE Hackathon 2024," February 23, 2024, https://www.softserveinc.com/en-us/news/softserve-engineers-win-nato-tide-hackathon-2024 or https://archive.ph/Sxfc2

[70] NATO ACT, "Coalition Warrior Interoperability Exercise," NATO's Strategic Warfare Development Command, n.d., https://www.act.nato.int/our-work/exercises/coalition-warrior-interoperability-exercise/ or https://archive.ph/n6dEO

[71] Ministry of Defence of Ukraine, "Україна вкотре виступила на щорічних навчаннях НАТО із взаємосумісності – CWIX," July 11, 2023, https://www.mil.gov.ua/news/2023/07/11/ukraina-vkotre-vistupila-na-shhorichnih-navchannyah-nato-iz-vzaemosumisnosti-%E2%80%93-cwix/ or https://archive.ph/hMwjc

[72] NATO ACT, "Battlefield Innovation: Ukraine's DELTA System Paves the Way for Allied Interoperability at CWIX24," July 12, 2024, https://www.act.nato.int/article/delta-system-cwix/

[73] NATO in Ukraine, "Представники Центру інновацій Міністерства оборони України успішно виступили на щорічних навчаннях НАТО – CWIX.," July 7, 2023, https://archive.ph/GJrIp

[74] Kimberly Underwood, "NATO's Support of Ukraine's C4 Capabilities," *Signal*, December 7, 2023, https://archive.ph/nkzWn

At CWIX24, the Ukrainian Ministry of Defense also officially announced that Delta successfully integrated the Polish artillery fire control system TOPAZ.[75] Ukrainian Deputy Minister of Defense for Digital Development, Digital Transformations and Digitalization, Kateryna Chernogorenko, further contextualized that "the Ukrainian system successfully coped with the task and confirmed compatibility with many other NATO systems. This year, the DELTA system team successfully tested 5 different interoperability standards and passed all tests successfully."[76]

Delta's development history and NATO interoperability allows the platform to exchange situational awareness data across the land, sea, air, and cyber domains, as well as medical and logistical information with NATO member states. As of this writing it is unknown how deeply involved NATO and its members are in levering Delta to provide tactical guidance and strategic inputs to optimize Ukraine's battlefield management and strategic decision-making.

Figure 19: Delta representatives at CWIX 2024

Source: NATO ACT, "Battlefield Innovation: Ukraine's DELTA System Paves the Way for Allied Interoperability at CWIX24," July 12, 2024, https://www.act.nato.int/article/delta-system-cwix/

2.3 Dzvin (Дзвін) & Everest

When we trace the history of Delta, we must also talk about the automated military command and control system Dzvin (Дзвін-АС). Dzvin took its inspiration from the automated management system Mars (АСУ МАРС), which was developed by a Ukrainian company called IQusion. IQusion was part of the IT Intecracy Group, a Ukrainian IT consortium, which included companies such as InBase, Softline, and SGS.[77] Very little information is publicly available on MARS. What we do know is that back in 2015, Ostro wrote a news article on the MARS system noting that the "automated control system helps coordinate the actions of units, allows you to unite people and equipment into a single information space and is capable of broadcasting operational data on combat operations online. […] The developed software is installed on secure gadgets, where each soldier, sergeant or officer works with electronic [maps] in the formats they need. Data on the planned and actual tactical situation are applied to [the maps] using the tactical signs familiar to most. To make the information as accurate as possible, many sensors can be connected to the system - unmanned aerial vehicles, thermal imagers, rangefinders, GPS receivers and much more. The messaging function in the system is implemented in the form of a tactical chat (provides the exchange of text messages between specific users and groups of users), which eliminates errors when transmitting coordinates."[78] Taras Poruchnik, the designer of the MARS system, further elaborated that "the army's need for this technology today [2015] is huge, because MARS is able to significantly increase the efficiency of the use of troops without re-equipping [them] with new, expensive weapons. This is a real opportunity to create a significant advantage over the enemy, and, therefore, to save the lives and health of our soldiers."[79]

Open source is unclear as to what happened to MARS after 2015. The system was either discontinued for unknown reasons or was entirely absorbed into the Dzvin project. Taras Poruchnik, for example, went on to become the head designer of Dzvin, and companies like InBase,

[75] Міністерство оборони України, "Українська бойова система DELTA успішно інтегрувалася з польською системою управління артилерійським вогнем TOPAZ," July 1, 2024, https://www.mil.gov.ua/news/2024/07/01/ukrainska-bojova-sistema-delta/ or https://archive.ph/tiXu7

[76] Ibid.

[77] IQusion, "Про нас," n.d., https://iqusion.com/ua/about.html or https://web.archive.org/web/20240522094620/https://iqusion.com/ua/about.html; Ostro, "Компания IQusion разработала для армии Украины автоматизированную систему управления МАРС," July 2, 2015, https://www.ostro.org/ru/press-releases/kompanyya-iqusion-razrabotala-dlya-armyy-ukrayny-avtomatyzyrovannuyu-systemu-upravlenyya-mars-i191686 or https://archive.ph/UgtJA

[78] Ostro, "Компания IQusion разработала для армии Украины автоматизированную систему управления МАРС," July 2, 2015, https://www.ostro.org/ru/press-releases/kompanyya-iqusion-razrabotala-dlya-armyy-ukrayny-avtomatyzyrovannuyu-systemu-upravlenyya-mars-i191686 or https://web.archive.org/web/20240522144039/https://www.ostro.org/ru/press-releases/kompanyya-iqusion-razrabotala-dlya-armyy-ukrayny-avtomatyzyrovannuyu-systemu-upravlenyya-mars-i191686

[79] Ibid.

Softline, and SGS joined the Dzvin project as subcontractors to a company called Everest Limited LLC (ТОВ Евереста Лімітед).[80]

The story of Aerorozvidka and Everest started to collide in the Spring of 2016, after Aerorozvidka presented its Delta prototype to then President of Ukraine Petro Poroshenko. As Aerorozvidka's Yaroslov Gonchar explained to news outlet BIHUS, "that's how the Ukrainian legislation works. In order for the [Delta] software to be adopted [by the armed forces], it has to be submitted as an R&D project [to the Ministry of Defense]. [The Ministry of Defense] invited a representative of the Everest company, Yury Chubatyuk [President of Everest]. We were told that [Everest] is the only registered software R&D contractor in Ukraine. It will do the paperwork [for Delta] according to [the] R&D requirements and take a commission as a contractor. [Everest] send some people, we will tell them [what they need to know], [and then Everest will] pass on the knowledge. [Everest] told [us], 'yes, yes, [we] will do [it]!' But time went by, nothing was happening."[81] On December 30, 2016, Everest signed a contract with the Ukrainian Ministry of Defense for the development of Dzvin.[82]

In contrast to Aerorozvidka, Everest was a well-established player in Ukraine's IT sector back in 2016. The company was founded in 1992, and according to archival screencaps in the Wayback Machine, it started assembling and selling personal computers and servers under its own brand. In 1996 it signed contracts with AMD, Intel, Asus, Samsung, and LG. And one year later it became the first Ukrainian company to sign a contract with Microsoft.[83] According to its website, Everest is "a leader in the field of digital transformation, technological and engineering solutions. […] By combining technologies and products, we use the full range of possibilities of digital solutions for fast and large-scale implementation. […] Our multidisciplinary team consists of experts in digital strategy, industry solutions, business intelligence, cloud environments, cyber security, engineers and data specialists who can solve a wide variety of business challenges."[84] There is nothing on the Everest website that would indicate that they are defense contractor or have accumulated experience on working on military platforms. But, on January 10, 2017 – two weeks after signing the contract for Dzvin with the Ministry of Defense – Everest joined the newly formed Association of Ukrainian Defense Manufacturers (AUDM).[85]

Dzvin is one part of an automated unified combat control system the General Staff of the Armed Forces has been longing for. According to opk.com.ua, Dzvin is a "highly integrated, automated system of command and control of combat operations at the strategic, operational and partially tactical (brigade) level, which allows in semi-automatic and automatic modes to generate combat control documents, create and track map information, receive comprehensive data on [your] own troops, available intelligence, data on the enemy troops, their current and prospective support, as well as carry out calculations of the ratio of forces and means, the optimality of their use in various scenarios."[86] The other two parts of the unified command and control system are ACS Prostir (АСУ Простір), developed by Telekart-Prylad (Телекарт-Прилад), and Oreanda-PS (Ореанда-ПС) created by Aerotechnika (Аеротехніка).[87] Both companies are also members of AUDM. Prostir is an automated tactical control and sensing system whose creation started in 2010. On the lower level it consists of infantrymen equipped with digital radios and PDAs, and data, communication, and sensor equipment installed in armored vehicles. At its heart lies a battle management system to oversee and coordinate combat preparation and execution. Telekart-

---

[80] InBase, "Контролює ситуацію на полі бою: експерт Олег Жданов розповів, як працює Дзвін-АС," December 10, 2022, https://web.archive.org/web/20230327082723/https://inbase.com.ua/ua/blog/kontroliuie-sytuatsiiu-na-poli-boiu-ekspert-oleh-zhdanov-rozpoviv-iak-pratsiuie-dzvin-as.html; Sofline, "В Україні прийнято на озброєння автоматизовану систему управління 'Дзвін-АС'," December 8, 2022, https://web.archive.org/web/20230327082812/https://softline.ua/ua/news/v-ukraini-pryiniato-na-ozbroiennia-avtomatyzovanu-systemu-upravlinnia-dzvin-as.html; SGS, "«Міноборони» робить важливі кроки на шляху цифрової трансформації війська," December 9, 2022, https://web.archive.org/web/20230327082802/https://www.sgs4business.com/news/minoboroni-robit-vazlivi-kroki-na-slahu-cifrovoi-transformacii-vijska.html; Note: It is unclear whether the Intecracy Group as a whole joined the Dvzin project or just a handful a companies.

[81] BIHUS, "The Army Wasted 600 Million? Failure of the Most Important Defense IT-project," *Youtube*, March 15, 2021, https://www.youtube.com/watch?v=hbSowbD1OZw, timestamp: 07:34

[82] МІНІСТР ОБОРОНИ УКРАІНИ, "До: 234/4341 від 18.12.2020 (Департамснт внугрішнього аудиту Міыістерства обороии Украіыи) Гепсрал-полковиику ХОМЧАКУ Р.Б. Оргаиізувати роботу щодо виконання пропозицій. Адміралу Полковнику Полковпыку юстиції Генерал-лейтенанту За нанркаістю врахуватн результати аудитів у …," December 18, 2020 https://drive.google.com/file/d/1c0ak7td9OyUWn-sYHCwJErFlBN_Tp_7EM/view, p. 7

[83] Everest, "history of the company," March 2, 2017, https://web.archive.org/web/20170302105103/http://www.everest.ua/, see: 'о компании [about company]' then 'История компании [history of the company]'

[84] Everest, "ПРО КОМПАНІЮ," January 16, 2022, https://web.archive.org/web/20220116111004/https://www.everest.ua/pro-nas/

[85] AUDM, "Рсстр підприемств Асоціації станом на," December 17, 2019, https://audm.org.ua/wp-content/uploads/Reyestr-chleniv-spilki.pdf or https://web.archive.org/web/20240522122032/https://audm.org.ua/wp-content/uploads/Reyestr-chleniv-spilki.pdf

[86] ОРК, "ЦИФРОВИЙ ВИМІР ЗСУ. ЗА ЯКИХ УМОВ ЦЕ МОЖЛИВО?" November 25, 2019, https://opk.com.ua/цифровий-вимір-зсу-за-яких-умов-це-можл/ or https://web.archive.org/web/20240522122207/ https://opk.com.ua/цифровий-вимір-зсу-за-яких-умов-це-можл/

[87] ОРК, "ЦИФРОВИЙ ВИМІР ЗСУ. ЗА ЯКИХ УМОВ ЦЕ МОЖЛИВО?" November 25, 2019, https://opk.com.ua/цифровий-вимір-зсу-за-яких-умов-це-можл/ or https://web.archive.org/web/20240522122207/ https://opk.com.ua/цифровий-вимір-зсу-за-яких-умов-це-можл/

Prylad was founded in Odesa in 2001. The company describes itself as "a leading national manufacturer of modern digital means of communication, telecommunication equipment, electricity metering devices, car parking systems."[88] While Telekart's does not sound like your typical defense contractor, it has done quite some work for the Ukrainian Armed Forces in the area of communications equipment.[89]

Figure 20-22: Dzvin platform

Source: (left) Defense Express, "ЦИФРОВИЙ ВИМІР ЗСУ (ВІДЕО)," *defence-ua*, Nov. 29, 2019, https://old.defence-ua.com/index.php/statti/9021-tsyfrovyy-vymir-zsu-video or https://archive.ph/JYGX8; (center) AUDM, "Асоціація виробників озброєння та військової техніки України спростовує розповсюджену неправдиву інформацію стосовно результатів виконання ДКР, шифр «ДЗВІН-АС»," March, 23, 2021, https://audm.org.ua/news/asotsiatsiya-virobnikiv-ozbroyennya-ta-vijskovoyi-tehniki-ukrayini-sprostovuye-rozpovsyudzhenu-nepravdivu-informatsiyu-stosovno-rezultativ-vikonannya-dkr-shifr-dzvin-as/ or https://archive.ph/HU8pQ; (right) ВІТАЛІЙ МАНЬКО, "Фактчекінг матеріалу Бігуса про "Дзвін-АС": 10 епізодів спецоперації проти ЗСУ," *Hvylya.net*, March 22, 2021, https://hvylya.net/analytics/227434-faktcheking-materialu-bigusa-pro-dzvin-as-10-epizodiv-specoperaciji-proti-zsu or https://archive.ph/9txzR

Oreanda by contrast "integrates aviation management complexes, radio engineering and aviation intelligence, as well as means of destruction and control points."[90] Essentially, it is an automated, unified airspace control solution, that aims to integrate all aviation and air defense assets from across Ukraine's armed forces. Aerotechnika, the company that developed Oreanda-PS, was established in 1991 by graduates from the Kyiv Radio Engineering School of Air Defense. The company specializes in automated air traffic control systems, radar systems, and it upgrades surface-to-air missile systems. Aerotechnika is a classic defense contractor with decades of military experience.

From December 2016 onward, Dzvin passed all its tests, military training exercises, and quality assurance sign offs during all the commission meetings with the General Staff of the Armed Forces. By all accounts, the system was working, and the General Staff was satisfied with its performance. The Ministry of Defense was largely kept out of the loop – even though it was the party that actually signed the contract with Everest.
Sometime in 2020, defense minister Andriy Taran ordered an internal audit of the Dzvin system. Among the delegation of experts conducting the first MoD audit were three representatives from military unit A2724 – including Delta developer Serhii Halchynskyi.

* * * *

In early-2020, the Main Directorate of Communications and Information Systems of the General Staff of the Armed Forces of Ukraine (Головне управління зв'язку та інформаційних систем ГШ ЗСУ) was reorganized and split into two separate parts. The Communications and Cyber Security Forces Command (Командування Військ зв'язку та кібербезпеки ЗС України) and the Central Department of Communications and Information Systems (Центральне управління зв'язку та інформаційних систем ГШ ЗС України).[91] Aerorozvidka – then military unit A2724 – was moved into the Communications and Cyber Security Forces Command.

A few months after this move, military unit A2724 was suddenly disbanded on the orders of then Chief of the General Staff and head of the Armed Forces, Ruslan Khomchak.[92] Yevhen Stepanenko, Commander of the Communications and Cyber Security Forces Command explained the decision by stating that "the legendary unit Aerorozvidka" was to be partitioned and its different

[88] Telecard, "Telecard," n.d., https://telecard.odessa.ua/ or https://web.archive.org/web/20240522122236/https://telecard.odessa.ua/

[89] Ukrmilitary, "Оновлений пункт управління авіацією від «Телекарт-Прилад»," December 16, 2019, https://www.ukrmilitary.com/2019/12/skp11.html or https://web.archive.org/web/20240522124318/https://www.ukrmilitary.com/2019/12/skp11.html; Ukrmilitary, "Радіостанція короткохвильова Р-1150," September 2, 2015, https://www.ukrmilitary.com/2015/09/radiostancya-R1150.html or https://web.archive.org/web/20240522124212/https://www.ukrmilitary.com/2015/09/radiostancya-R1150.html

[90] ОРК, "ЦИФРОВИЙ ВИМІР ЗСУ. ЗА ЯКИХ УМОВ ЦЕ МОЖЛИВО?" November 25, 2019, https://opk.com.ua/цифровий-вимір-зсу-за-яких-умов-це-можл/ or https://web.archive.org/web/20240522122207/ https://opk.com.ua/цифровий-вимір-зсу-за-яких-умов-це-можл/

[91] Микола Федорків, "Командувач Військ зв'язку та кібербезпеки ЗСУ: про зміни у структурі військ, головні функції та «Об'єднані зусилля – 2020»," *Armyinform*, September 17, 2020, https://armyinform.com.ua/2020/09/17/komanduvach-vijsk-zvyazku-ta-kiberbezpeky-zsu-pro-zminy-u-strukturi-vijsk-golovni-funkcziyi-ta-obyednani-zusyllya-2020/ or https://archive.ph/tTyVK

[92] Ibid.

parts to be integrated into other military structures.[93] The primary reason given for this move was that over the years Aerorozvidka had taken on an excessive workload of other things (ex. maintaining its own financial management system, record keeping, and coordinating efforts with intelligence and military units etc.) that were supposedly distracting the unit from its main combat tasks.[94] As a result, the air reconnaissance and surveillance parts of unit A2724 were integrated into existing intelligence units, and A2724's IT people were moved into units working on communication and cyber security.[95] Aerorozvidka was torn apart.

Yaroslav Gonchar was transferred from the General Staff to the newly formed Communication and Cyber Security Forces Command. According to Gonchar, the Command then told him that there were no open positions that corresponded to his professional qualifications. He was then unceremoniously released from the armed forces.[96] In the fall of 2020, Gonchar and others got together to recreated Aerorozvidka outside the armed forces as a non-governmental organization: Aerorozvika NGO.

* * * *

On December 14, 2020, the Ministry of Defense concluded its auditing report on 'the developments of automation systems for the armed forces within the period from January 1, 2016, to December 1, 2020.' News outlet BIHUS eventually got their hands on the document and aired a 30-minute-long segment on March 15, 2021.[97] BIHUS prominently included interviews with Yaroslav Gonchar and Serhii Halchynskyi. According to the MoD's report, the Dzvin system had major deficiencies and did not work as promised. The report outlined that the system was (1) incompatible with NATO standards – meaning it was impossible to exchange information and data with NATO systems, and new equipment and assets imported from NATO countries could not be easily integrated; (2) Dzvin's digital map was not based on a shared data environment. Instead, information was siloed within the system, and maps could not be edited by individual units. BIHUS compared Dzvin's setup to users continuously creating new Word documents that had to be shared via E-mail, rather than a co-working space in line with Google Docs; (3) The system also did not automatically segment classified information by leveraging data access controls. Instead, three different computer networks were created for each security classification level. To transfer information from one classification level to another, operators would literally use USB sticks to copy the data.

The auditing report was partially derived from the findings of a military commission visit during which Everest presented the final Dzvin system. As Halchynskyi explained to BIHUS, "as soon as we entered, we felt we weren't welcome. Other commission members whispered to each other behind our backs. And representatives of the contractors were always nearby." BIHUS goes on to note that according to Halchynskyi, "Everest did not let them near the centerpiece, the code. When they finally saw the code, the guys discovered the problems. And they made a list of the flaws." As Halchynskyi states, "it is very important for these things to be listed in the protocol as flaws, because this means that the contractor is obliged to correct them or will be fined." However, the commission and the head of the commission eventually turned 'flaws' into mere 'suggestions,' which the contractor was not obliged to fix at all. In the end, the commission pushed forward the acquisition of Dzvin and signed off on a project that by now had cost approximately 620 million Ukrainian hryvnia (approximately 22 million USD).

The release of the audit report led the MoD to immediately halt the acquisition and stop any further funding of the Dzvin system. The MoD also informed the State Bureau of Investigations (Державне Бюро Розслідувань) to scrutinize the Dzvin project for potential corruption. On November 3, 2022, the National Anti-Corruption Bureau of Ukraine (Національне Антикорупційне Бюро України) opened its own investigation into Dzvin.[98] In response to the BIHUS segment and the MoD's audit report, AUDM released a firm statement on March 23, 2021, accusing the MoD's auditing department of clear bias, not examining relevant documents and software code, and it blamed the press for conducting a coordinated campaign

[93] Ibid.

[94] Ibid.

[95] Ibid.

[96] Юрій Бутусов, "Підполковник Ярослав Гончар: "Лобісти "Дзвону" в ЗСУ хочуть оцифрувати радянську армію і виставити за реформу корупцію та показуху. Нецільові витрати по ДКР "Дзвін" - 160 мільйонів"," *censor.net*, March 4, 2021, https://censor.net/ru/resonance/3251465/pdpolkovnik_yaroslav_gonchar_lobsti_dzvonu_v_zsu_hochut_otsifruvati_radyansku_armyu_vistaviti_za_reformu or https://web.archive.org/web/20240522124728/https://censor.net/ru/resonance/3251465/pdpolkovnik_yaroslav_gonchar_lobsti_dzvonu_v_zsu_hochut_otsifruvati_radyansku_armyu_vistaviti_za_reformu

[97] BIHUS, "The Army Wasted 600 Million? Failure of the Most Important Defense IT-project," Youtube, March 15, 2021, https://www.youtube.com/watch?v=hbSowbD1OZw

[98] Олена Чернишова, "По кому подзвін. Міноборони взяло на озброєння скандальну систему «Дзвін» — що цьому передувало," January 5, 2023, https://dou.ua/lenta/articles/dzvin-system-in-army/ or https://web.archive.org/web/20240522125057/https://dou.ua/lenta/articles/dzvin-system-in-army/; Yaroslav Yurchyshyn, "НАБУ розслідує розкрадання в особливо великих розмірах на військовій системі "Дзвін", яку в Міністерство оборони України чомусь вперто готують до постачання в Збройні Сили України / The Armed Forces of Ukraine," Facebook, November 22, 2022, https://archive.ph/52W6H

against Dzvin and the General Staff of the Armed Forces.[99] Several people working on Dzvin also published their own op-eds, including Taras Poruchnyk (head designer of Dzvin) and Victor Valeev (director of the association Ukraine IT - which includes Softline – a subcontractor working on Dzvin), to disprove the findings of the audit report.[100] Everest also sued the MoD in Kyiv's Commercial Court for breach of contract.[101]

Curiously, on December 6, 2022, then Ukrainian Minister of Defence Oleksiy Reznikov, signed an order to adopt Dzvin into the Armed Forces.[102] As Reznikov explained one day later on Facebook, "currently, all formal procedures have been completed, the strategic-level [automated control system] has officially joined the ranks and will work in the interests of the Armed Forces. Next, the General Staff will make decisions regarding the scaling parameters of this [automated control system]."[103] In the same Facebook post, Reznikov also noted that "in addition, the Ministry of Defense received a positive expert opinion regarding the 'Delta Integration Platform' special software complex. This is an important stage in the formalization of the platform according to the approved roadmap. Next, a cycle of official tests will take place, based on the results of which a decision will be made on adoption."[104]

Looking from the outside in – and not having access to the Dzvin system – this CSS cyber defense report cannot provide an evaluation on whether the accusations against Dzvin are true or false. What is evident however, is that there was clear infighting between the General Staff of the Armed Forces on the one hand, and the MoD on the other. According to Ihor Kolesnyk, former deputy chief of the General Staff, this institutional tension has existed since at least 2005.[105] Similarly, Everest and Aerorozvidka are clearly not getting along either, and Dzvin and Delta are likely going to be everlasting competitors. For this infighting and potential corruption case to occur while Ukraine is stemming an invasion, is of particular concern. Reznikov's decision to move forward with both platforms seems to have been the most prudent and face-saving way forward. But – if the allegations against Dzvin are true – then Reznikov's decision might likely run the risk of deploying a potentially chaotic automated command-and-control system while the country is fighting for its survival.

Writing for Hvyla.net in 2020, Yuri Radchenko noted that when it comes to the realities in Ukraine, the competition is not so much technological. It is "simply a war of destruction by business groups using officials, the media, and law enforcement as their tools."[106] It is not entirely clear whether Radchenko's analysis holds true for the case at hand. As a volunteer group, Aerorozvidka seems to behave distinctly different from the persistent power struggles among Ukraine's private sector companies. And as Aerorozvidka noted on Facebook on October 8, 2021, "the criminal decisions that were taken to destroy our achievements, ecosystem and subjectivity in the format of the A2724 military unit will not be forgotten. We emphasize that this was done with the aim of concealing a crime that is still being investigated by the SBU. We will not stop and make efforts so that these shameful events become a lesson and conclusions are drawn for future generations."[107] What does ring true however, is that the miltech competition in wartime Ukraine was and probably is still a problem. Ruslan Prylypko, head of Aerorozvidka NGO's IT department, explained that "competition is good when there is something to compete for. In [Ukraine's] case, a lot of effort is spent inefficiently. […]

---

[99] AUDM, "The Association of Ukrainian Defense Manufacturers denies the spread false information about the results of the implementation of the R&D, code "DZVIN-AS"," March 23, 2021, https://audm.org.ua/en/news/asotsiatsiya-virobnikiv-ozbroyennya-ta-vijskovoyi-tehniki-ukrayini-sprostovuye-rozpovsyudzhenu-nepravdivu-informatsiyu-stosovno-rezultativ-vikonannya-dkr-shifr-dzvin-as/ or https://web.archive.org/web/20240522125349/https://audm.org.ua/en/news/asotsiatsiya-virobnikiv-ozbroyennya-ta-vijskovoyi-tehniki-ukrayini-sprostovuye-rozpovsyudzhenu-nepravdivu-informatsiyu-stosovno-rezultativ-vikonannya-dkr-shifr-dzvin-as/

[100] ТАРАС ПОРУЧНИК, "Чув «Дзвін» та не знаю де він," *Hvylya*, March 25, 2021, https://hvylya.net/analytics/227610-chuv-dzvin-ta-ne-znayu-de-vin or https://web.archive.org/web/20240522125820/https://hvylya.net/analytics/227610-chuv-dzvin-ta-ne-znayu-de-vin; ТАРАС ПОРУЧНИК, "Чув «Дзвін» та не знаю де він-2. Як маніпулює команда Бігуса," *Hvylya*, April 5, 2021, https://hvylya.net/analytics/228257-chuv-dzvin-ta-ne-znayu-de-vin-2-yak-manipulyuye-komanda-bigusa or https://web.archive.org/web/20240522125802/https://hvylya.net/analytics/228257-chuv-dzvin-ta-ne-znayu-de-vin-2-yak-manipulyuye-komanda-bigusa; Віктор Валєєв, "АСУ «Дзвін-АС»: інформація про проблеми системи є фейком," Softline, June 30, 2021, https://www.softline.kiev.ua/news/asu-dzvin-as-informatsiia-pro-problemy-systemy-ie-feikom.html or https://web.archive.org/web/20240522125908/https://www.softline.kiev.ua/news/asu-dzvin-as-informatsiia-pro-problemy-systemy-ie-feikom.html

[101] Commercial Court of Kyiv City, "Господарський суд міста Києва в порядку статей 120-121 Господарського процесуального кодексу України, по справі № 910/19348/20, - за позовом Товариства з обмеженою відповідальністю "Еверест Лімітед" до Міністерства оборони України," youcontrol.com.ua, May 17, 2012, https://youcontrol.com.ua/en/catalog/court-document/96926197/ or https://archive.ph/SVyPF

[102] Резніков Олексій, "У публічному просторі багато інформації про вражаючі результати застосування важкої зброї натівських зразків нашими воїнами," Facebook, December 8, 2022, https://archive.ph/KfqKu

[103] Ibid.

[104] Ibid.

[105] Роман Пагулич, "Чому українські воєначальники конфліктують між собою під час війни?" Radiosvoboda, August 2, 2021, https://www.radiosvoboda.org/a/konflikt-tarana-ta-homchaka-i-zryv-doz/31385826.html or https://web.archive.org/web/20240522130607/https://www.radiosvoboda.org/a/konflikt-tarana-ta-homchaka-i-zryv-doz/31385826.html

[106] Юрій Радченко, "Кому вигідно?" *Hvylya.net*, October 15, 2020, https://archive.ph/rmBSg

[107] Аеророзвідка, "Ніщо не спинить ідею час якої настав," October 8, 2021, https://archive.ph/Vm8RB

The state should not control, but help. Reduce barriers and allow those who really have the expertise to join the teams that develop it.[108]

2.4 Center for Innovation and Development of Defense Technologies

In October 2021, the Ministry of Defense and the General Staff of the Armed Forces signed a joint directive to establish the Center for Innovation and Development of Defense Technologies within the MoD (Центром інновацій та розвитку оборонних технологій Міністерства оборони України). In its announcement, the MoD noted that "we have resuscitated the projects of automated combat control systems and found solutions for the future of automated control systems of the operational and strategic level, tactical level, and situational awareness system."[109] Serhii Halchynskyi and others who worked on the Delta system were moved into the new Center. The Center is now responsible for maintaining and further developing Delta.

An article by Maria Brovinska for dev.ua shows the variety of talent that were transferred to the new Center. They include Maksym Korzhenevskyi, founder of the IT company MK-Consulting. Maksym never served in the armed forces and when mobilized as a volunteer was eventually placed within the Center. As Maria puts it, "when [Maksym] arrived, he offered the command a project related to Computer Vision/[machine learning]/Neural Network. Received consent, resources, support. Several more projects were launched in the process. There are such tasks that come from the command, but initiative is more valued [in the Center]: [You] come up with something, develop a proof of concept, show it to management, receive approval and support – and you move on."[110] Then there is Mykola Matiychuk, a game developer. As Maria explains, "Mykola was not given a machine gun and a helmet, but a laptop, a mouse and a monitor. And a mobile phone for one of the tasks. His colleagues are not combatants, but programmers, devops, [and] analysts."[111] Alexander, an android engineer, was supposed to remain in the reserve force because he was a key employee at bank. Instead, he went to the front and started working on developing several Android applications to improve intelligence operations, including application[s] for encryption, object detection, and drones. With the approval of his commander his small team was eventually transferred to the Center.[112] As Alexander put it "when I got here, I realized that today's army is very different from the army of 2014, and our IT skills will be needed."[113]

In October 2023, representatives from the Center took part in the React+TS FWDAYS'23 conference in Kyiv and publicly revealed for the first time that Delta was used to plan and coordinate the sinking of the Russian Black Sea flagship *Moscva* in April 2022, and the 2022 counter-offensive in the Kherson and Mykolaiv oblast.[114] The Center's representatives also noted that Delta was used to plan the attack on the Kerch bridge, but open source is unclear whether this was in reference to the October 2022 truck bombing or the July 2023 sea drone attack.

3 Aerorozvidka NGO

When Russia invaded Ukraine on February 24, 2022, Aerorozvidka NGO stood up its first situational awareness center in Kyiv, and the Ukrainian MoD deployed the Delta system on a cloud server in Ukraine in preparation for defending the capital. As Aerorozvidka NGO explained it, "we organized the first situational center in Kyiv within a few days of the start of the full-scale invasion. Interacting with the military-civilian administration of Kyiv, the team of the situational center formed a comprehensive picture

[108] Таїса Мельник, "«Цифровізація в армії ще не починалася». Керівник ІТ-напряму «Аеророзвідки» про експорт Delta, $50 млн на фронтову кібербезпеку та ленд-ліз для інновацій," Forbes Ukraine, April 24, 2023, https://web.archive.org/web/20240522084007/https://forbes.ua/innovations/tsifrovizatsiya-v-armii-shche-ne-pochinalasya-kerivnik-it-napryamku-aerorozvidki-pro-eksport-delta-50-mln-na-frontovu-kiberbezpeku-ta-lendliz-dlya-innovatsiy-24042023-13182

[109] Міністерство оборони України, "В Міноборони створено Центр інновацій та оборонних технологій: відповідну спільну Директиву підписали Міністр оборони України та Головнокомандувач Збройних Сил України," October 2021, https://www.mil.gov.ua/special/news.html?article=64623 or https://web.archive.org/web/20240522130851/https://www.mil.gov.ua/special/news.html?article=64623

[110] Марія Бровінська, "ІТ-служба в ЗСУ та перевод з інших підрозділів - міф чи реальність? 4 вдалих приклади із лайфхаками та порадами," *Dev.ua*, May 18, 2022, https://dev.ua/news/zsu-aitishnyky-1652849247 or https://web.archive.org/web/20240522131407/https://dev.ua/news/zsu-aitishnyky-1652849247

[111] Ibid.

[112] Ibid.

[113] Ibid.

[114] Armyinform, "Творці системи DELTA презентували її на найбільшій технічній конференції в Україні," October 27, 202, https://armyinform.com.ua/2023/10/27/tvorczi-systemy-delta-prezentuvaly-yiyi-na-najbilshij-tehnichnij-konferencziyi-v-ukrayini/ or https://web.archive.org/web/20240522131450/https://armyinform.com.ua/2023/10/27/tvorczi-systemy-delta-prezentuvaly-yiyi-na-najbilshij-tehnichnij-konferencziyi-v-ukrayini/

of the state of the infrastructure of the city and region. Coordination between checkpoints and patrols was also established to avoid conflicts due to the use of UAVs and the movement of crews near the location of Ukrainian units. The collected information was used to plan the actions of defenders, to establish effective cooperation between different units, as well as to form an operational picture for the leadership of the Ministry of Defense and the military-civilian administration of Kyiv city."[115]

Figure 23: Aerorozvidka NGO logo

The defense of Kyiv was the starting point for the rapid growth of Delta users and the steadfast collaboration between Aerorozvidka NGO and numerous military units that pushed the adoption of a concept known as network-centric warfare.

The idea of network-centric warfare (NWC) was developed in the US back in the late 1990s to conceptualize how the US Armed Forces ought to organize and fight in the Information Age. Part of the equation was for the military to achieve information superiority, i.e. "the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting and/or denying an adversary's ability to do the same."[116] Network centric warfare is the mean to operationalize information superiority on the tactical battlefield. US military thinking thus went on to define network-centric warfare as, "an information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization. In essence, NWC translates information superiority into combat power by effectively linking knowledgeable entities in the battlespace."[117] That being said, turning NWC into a practical reality on the tactical battlefield, is a never-ending evolutionary process that – among countless other items – necessitates the constant adoption of new technologies and deployment of sensors, perpetual investments in experimental military capabilities, ceaselessly tapping into new talent pools, and continuously restructuring organizational processes and information flows.

Aerorozvidka itself describes network-centric warfare (sometimes also simply equated to ISTAR – intelligence, surveillance, target acquisition and reconnaissance) as following: "We often repeat that a small Soviet army cannot defeat a large Soviet army. The key to our victory is the transition to network-centric rules of warfare, which provide an advantage over the enemy thanks to complete information awareness, where every soldier can get the information he needs. And therefore, after February 24, we began to implement a network-centric approach, which includes opening situational centers that provide situational awareness for all security and defense sector representatives."[118]

One – if not the most important – base requirement for network-centric warfare is a reliable, resilient, and fast way to get data from A to B. The ViaSat hack on the eve of the Russian invasion severely disrupted Ukraine's premier internet satellite communication connection link (more on this in section on Tooway). In parallel, Russian Armed Forces shelled Ukrainian cell towers, electricity infrastructure, cut fibre optic cables, and took over Internet Service Providers in the occupied territories.[119] Speaking to Euronews in April 2024, Stanislav Prybytko, Director-General of the Directorate for mobile broadband within Ukraine's Ministry of Digital Transformation, summarized that "Russia has destroyed over 4,300 mobile base stations and a quarter of the country's internet networks since February 2022. The country's fibre optic network has also been impacted, with more than 30,000 km of cables spread out throughout Ukraine damaged or destroyed in the fighting so far."[120] Writing for Telegeography, Tim Stronge aptly summarized that "when physical network problems do occur, satellite communications can shine."[121] As such, Ukraine was incredibly fortunate that a simple Twitter exchange between Ukraine's Minister for

[115] Aerorozvidka, "Situational awareness is the key to our victory," n.d., https://aerorozvidka.ngo/situational-awareness/ or https://archive.ph/0Vi71

[116] US Joint Chiefs of Staff, "Joint Publication 3-13: Joint Doctrine for Information Operations," October 19, 1998, p. I-10, https://nsarchive.gwu.edu/document/17604-joint-chiefs-staff-joint-publication-3-13

[117] David Alberts, John Garstka & Frederick Stein, "Network Centric Warfare – Developing and Leveraging Information Superiority," DoD C4ISR Cooperative Research Program (CCRP), May, 1999, https://apps.dtic.mil/sti/tr/pdf/ADA406255.pdf

[118] Aerorozvidka, "The year of unbreakability Aerorozvidka Chronicles," n.d., https://aerorozvidka.ngo/the-year-of-unbreakability/ or https://archive.ph/Xx7XM

[119] Vera Bergengruen, "The Battle for Control Over Ukraine's Internet," *Time*, October 18, 2022, https://time.com/6222111/ukraine-internet-russia-reclaimed-territory/; Adam Satariano & Scott Reinhard, "How Russia Took Over Ukraine's Internet in Occupied Territories," *The New York Times*, August 9, 2022, https://www.nytimes.com/interactive/2022/08/09/technology/ukraine-internet-russia-censorship.html

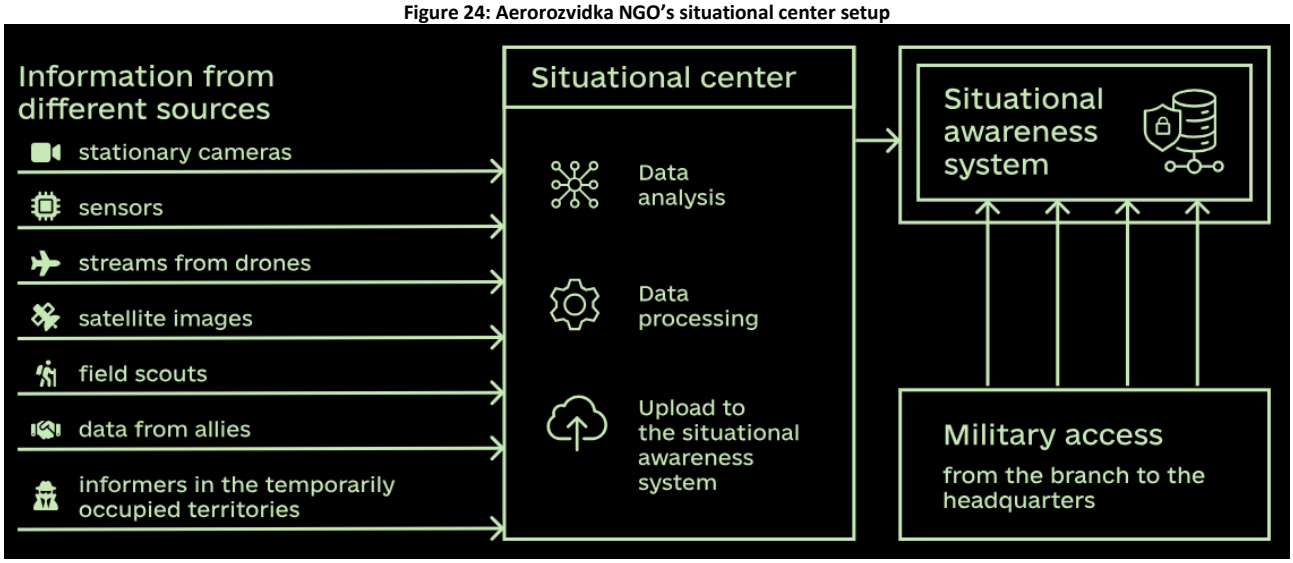
[120] Anna Desmarais, "Ukraine facing €4.38 billion post-war bill to restore telecom industry crippled by Russian attacks," *Euronews*, April 23, 2024, https://www.euronews.com/next/2024/04/23/ukraine-facing-438-billion-post-war-bill-to-restore-telecom-industry-crippled-by-russian-a

[121] Tim Stronge, "What to Know About Fiber's Role in Ukraine's Information War," *Telegeography*, March 1, 2022, https://blog.telegeography.com/what-to-know-about-fibers-role-in-ukraines-information-war

Digital Transformation Mykhailo Federov and SpaceX owner Elon Musk two days after the invasion, resulted in the shipment of hundreds of Starlink terminals to Ukraine during the early days of the battle of Kyiv on February 28, 2022. Without Starlink, everything from Delta's cloud deployment to Aerorozvidka's situational centers, and the massive amounts of data streamed from drones and stationary cameras could not have been share and analyzed in the speed and manner that was so crucial to the defense of the capital.

As of this writing, Aerorozvidka NGO maintains nine situational awareness centers in the frontline Oblasts of Chernihiv, Donbas, Kharkiv, Kherson, Kryvyi Rih, Kyiv, Mykolaiv, Sumy, and Zaporizhzhia. All centers are nomadic in nature and have been moved multiple times during the war. Each center consists of 20-25 civilian and military operatives that must undergo polygraph tests administered by the SBU's department for military counterintelligence or were vouched for by a trusted person/military unit. The military operatives receive their salary from the state, while the civilian operatives are directly employed by Aerorozvidka NGO. The managerial hierarchy within each center dependents upon regional circumstances. Gonchar notes that, "if we need to involve the military from a certain part, then we do it by agreement with their leadership."[122] Aerorozvidka's situational awareness centers are essentially technological hubs that collect intelligence, and fuse and coordinate technical means to conduct joint operations. On the collection part, the centers absorb information from stationary cameras, sensors, drone footage, operatives in the field (incl. walk-in informants), open-source intelligence, and data provided to them by partners (ex. satellite imagery) which is fed into Delta. Within each center there is a clear division of who is responsible for what. Analysts that work with informants only work with them; they will not be tasked to – for example – input satellite imagery data. In an interview with Forbes.ua, Aerorozvidka NGO's Ruslan Prylypko also touched upon the use of AI: "For example, to review a drone flight and find enemy equipment. You uploaded a video, a neural network watches it, and says that it is highly likely that this object is a car, with a concentration of manpower. Another network analyzes whether there was a command post or a militant group warehouse. This is one of the cases. There are several in the works."[123]

Figure 24: Aerorozvidka NGO's situational center setup



Source: Aerorozvidka, "Situational Awareness is the key to victory," *aerorozvidka.ngo*, n.d., https://aerorozvidka.ngo/situational-awareness/ or https://archive.ph/0Vi71

To underpin the work of the situational awareness centers, Aerorozvidka NGO also offers drone piloting courses, Starlink frontline-use training, and lessons on how to operate Delta.

Since 2017/19, Aerorozvidka NGO has also been producing its own custom-built drone, the R18 octocopter, with some parts being domestically manufactured, 3D printed,

[122] Maria Gurska, "«На основі нашої роботи ухвалюють воєнні рішення». Як працюють ситуаційні центри «Аеророзвідки» та чим система «Дельта» схожа на стрічку у Twitter," Dou.ua, February 6, 2023, https://dou.ua/lenta/interviews/air-intelligence-situational-centers/ or https://web.archive.org/web/20240522132002/https://dou.ua/lenta/interviews/air-intelligence-situational-centers/

[123] Таїса Мельник, "«Цифровізація в армії ще не починалася». Керівник IT-напряму «Аеророзвідки» про експорт Delta, $50 млн на фронтову кібербезпеку та ленд-ліз для інновацій," Forbes Ukraine, April 24, 2023, https://web.archive.org/web/20240522084007/https://forbes.ua/innovations/tsifrovizatsiya-v-armii-shche-ne-pochinalasya-kerivnik-it-napryamku-aerorozvidki-pro-eksport-delta-50-mln-na-frontovu-kiberbezpeku-ta-lendliz-dlya-innovatsiy-24042023-13182

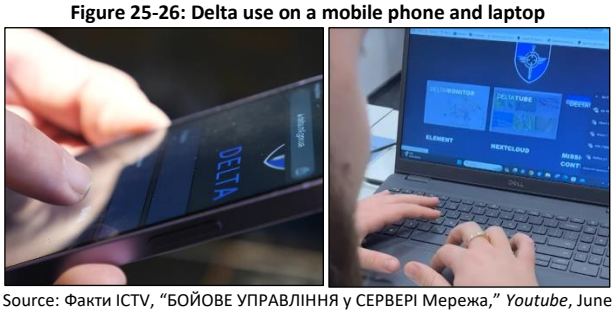
or imported from China.[124] According to a June 2022 article by Forbes, the R18 can fly for up to 40 minutes, carry a payload of maximum five kilograms, and costs Aerorozvidka around 20.000 USD to manufacture.[125]

Some – if not all – of the 3D printed parts are supplied to Aerorozvidka by the 3D Print Army (ДрукАрмія), which is a 6000+ member strong Ukrainian 3D printer owner community co-founded by Ukrainian blogger and Youtube personality Yevhen Volnov (aka. Major Chornobaiev).[126] The 3D Print Army's website notes that the community has ~7.500 3D printers at its disposal and is manufacturing on-demand custom parts for numerous Ukrainian military units free of charge.[127]

4 Delta & Cybersecurity

To get a Delta account, an applicant must confirm his/her identity via one of three options. Option A: Through a guarantor – which is a user that already has access to Delta and is willing to confirm the applicant's identity and military unit. Option B: Through the Secure Electronic Documents Management System (SEDO-M). For this route, the headquarters or the military unit itself has to send a request for access to Delta on behalf of the applicant via SEDO-M. And in case neither of these two options are feasible, "the people responsible for verification at Delta will try to verify your identity using available means, but this will take much longer and is not guaranteed to be successful."[128] Concurrent to the identity confirmation process, an applicant also has to submit two photos – one photo of the applicant holding his open and readable passport, and another of the passport itself. The applicant must put all this information into the Delta registration form. Delta will contact the applicant within 1-2 days to clarify other details.

Figure 25-26: Delta use on a mobile phone and laptop



Source: Факти ICTV, "БОЙОВЕ УПРАВЛІННЯ у СЕРВЕРІ Мережа," *Youtube*, June 18, 2024, https://www.youtube.com/watch?v=61vPTrnOM4s

Nowadays, Delta automatically enables two-factor authentication (2FA) for all accounts. Previously it relied on SMS verification, but this approach has since been abandoned – possibly due to successful Russian smishing and SIM jacking attacks. In cooperation with Aerorozvidka NGO's Cyber Resilience Project, Delta's aim is to provide YubiKeys to all Delta users free of charge.[129] YubiKeys are hardware authentication devices which users can physically plug into their USB port. They replace receiving an authentication code via SMS or generating one via an authenticator app.[130] Ruslan Prylypko, head of Aerorozvidka NGO's IT department, elaborated that "a [Yubi]key costs an average of $50. The entire security and defense sector needs $50 million. We want every soldier to have an assault rifle, helmet, and bulletproof vest. Likewise, every military man has a digital space where he communicates and receives orders. And this environment must be protected. As long as this is not being done by the government in a targeted manner, we want to be the first for Delta users."[131] In case of technical emergencies, the Delta team also maintains a Signal and WhatsApp account.[132] Delta user have to agree to "undergo a polygraph (lie detector) test in the event of counterintelli-

[124] Euromaidan Press, "Ukraine's R18: the game-changing night drone shaping the front lines," Youtube, May 16, 2023, https://www.youtube.com/watch?v=5rHCJDJSfUw

[125] David Hambling, "How Ukraine Perfected The Small Anti-Tank Drone," *Forbes*, June 1, 2022, https://www.forbes.com/sites/davidhambling/2022/06/01/how-ukraine-perfected-the-small-anti-tank-drone/?sh=685d30ae3171

[126] Олексій Дзюба, "«Кудись виїхати і пропустити двіж їбаш#ти рус#ю? Ні-ні». Чому «Майор Чорнобаєв» долучився до створення «ДрукАрмії», яка вже витратила 25 млн грн на знищення окупантів," January 8, 2024, https://dev.ua/news/kudys-vyikhaty-i-propustyty-takyi-dvizh-ibashty-rusiu-ni-ni-chomu-maior-chornobaiev-doluchyvsia-do-stvorennia-drukarmii-iaka-vzhe-vklala-25-mln-hrn-v-znyshchennia-okupantiv or https://web.archive.org/web/20240522132021/https://dev.ua/news/kudys-vyikhaty-i-propustyty-takyi-dvizh-ibashty-rusiu-ni-ni-chomu-maior-chornobaiev-doluchyvsia-do-stvorennia-drukarmii-iaka-vzhe-vklala-25-mln-hrn-v-znyshchennia-okupantiv

[127] 3D Print Army website, n.d., https://drukarmy.org.ua/en or https://archive.ph/NCq6W

[128] Центр інновацій та розвитку оборонних технологій Міністерства оборони України "Реєстрація користувача," Delta Wiki, n.d., https://web.archive.org/web/20240522132225/https://delta.mil.gov.ua/wiki/monitor/registration/

[129] Центр інновацій та розвитку оборонних технологій Міністерства оборони України, "Двофакторна автентифікація," Delta Wiki, n.d., https://web.archive.org/web/20240522132548/https://delta.mil.gov.ua/wiki/monitor/mfa/; Aerorozvidka NGO, "Cyber resilience is a new challenge of network-centric warfare," n.d. https://web.archive.org/web/20240522132701/https://aerorozvidka.ngo/cyber-resilience/

[130] Jessica Lau, "What is a YubiKey and how does it work?" *Zapier,* November 27, 2023, https://zapier.com/blog/what-is-a-yubikey/

[131] Таїса Мельник, "«Цифровізація в армії ще не починалася». Керівник IT-напряму «Аеророзвідки» про експорт Delta, $50 млн на фронтову кібербезпеку та ленд-ліз для інновацій," Forbes Ukraine, April 24, 2023, https://archive.ph/NriaW

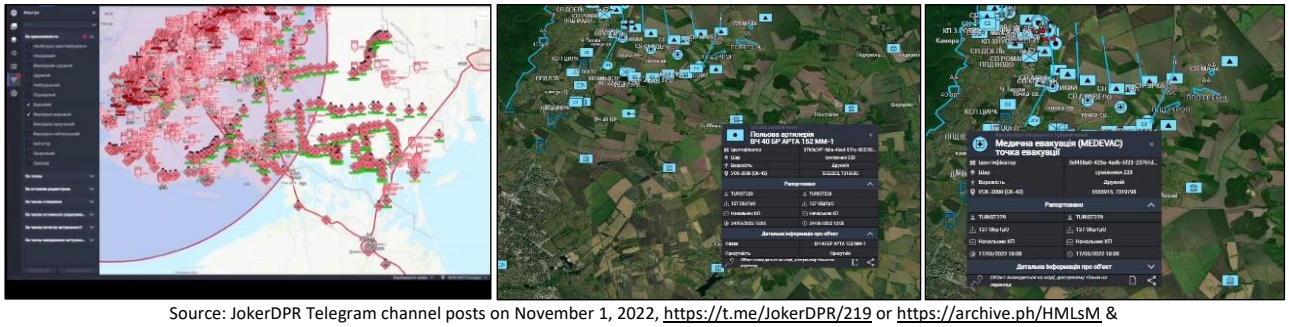
[132] Центр інновацій та розвитку оборонних технологій Міністерства оборони України, "Що таке DELTA?" Delta Wiki, n.d., https://web.archive.org/web/20230406115016/https://delta.mil.gov.ua/wiki/info/

gence activities and [are made] aware of the criminal liability in case of disclosure of information from the system to the enemy."[133]

According to Delta's own wiki, "from 2021, allied cyber units are constantly scanning the [Delta] system for vulnerabilities, intrusion attempts, data leaks, and more."[134] In an interview with dou.ua on February 6, 2023, Gonchar noted that "it must be admitted that the [Russian] phishing attacks were partially successful, they managed to intercept the account of one user in the Kharkiv [region]. There were no tragic consequences. The enemy was in the system for about 12 minutes. During this time, cyber defenders monitored the situation and removed access. But this interception coincided with the offensive of the Armed Forces, so the enemy could not use this information promptly. Then our Armed Forces counterattacked at a frantic pace, and the information available to the enemy became irrelevant the very next day."[135]

The Delta breach that Gonchar mentioned is in reference to the activity of a pro-Russian online persona named JokerDPR.[136] The acronym DPR likely stands for the Donetsk People's Republic. On November 1, 2022, JokerDPR posted a 3-minute-long video in his now 240.000 subscriber strong Telegram channel, showing him navigate inside the Delta system.[137] He explained that "my loyal followers of the Killnet hacker group really wanted to break into it, but dad did everything for you guys a long time ago. I decided to show you how DELTA works and looks from the inside. […] And I also changed the data there a little, rearranging different squares with rhombuses and other strange figures. But will you fix it? Sometimes paper maps are better."[138] Two days later, on November 3, JokerDPR posted a 16-minute-long video of him navigating inside the Delta system again.[139] In that post, JokerDPR highlighted that the breach occurred back in August 2022, and that he was particularly angry with Ukrainian war journalist Yuriy Butusov for spreading lies about the breach. According to JokerDPR, the breach was not the result of phishing, it did not last a mere 13 minutes, and it did not only concern the southern part of Ukraine – as Butusov claimed in a Facebook post on November 1.[140] JokerDPR then went on to claim that he infected several other Delta users through the Delta system itself (potentially by using the Element chat).[141]

Figure 27-29: JokerDPR's Delta breach



Source: JokerDPR Telegram channel posts on November 1, 2022, https://t.me/JokerDPR/219 or https://archive.ph/HMLsM & https://t.me/JokerDPR/209 or https://archive.ph/xjfkL

The JokerDPR persona (previously also known as JokerDNR) is a well-known social media figure in the Russia-Ukraine conflict.[142] It made its first appearance on October 21, 2019.[143] In a 2020 interview with TheRecord,

[133] Центр інновацій та розвитку оборонних технологій Міністерства оборони України "Правила безпеки використання СПЗ ІП "Дельта" (далі - система)," Delta Wiki, n.d., https://web.archive.org/web/20240522133137/https://delta.mil.gov.ua/wiki/info/security/

[134] Центр інновацій та розвитку оборонних технологій Міністерства оборони України, "Що таке DELTA?" Delta Wiki, n.d., https://web.archive.org/web/20230406115016/https://delta.mil.gov.ua/wiki/info/

[135] Maria Gurska, "«На основі нашої роботи ухвалюють воєнні рішення». Як працюють ситуаційні центри «Аеророзвідки» та чим система «Дельта» схожа на стрічку у Twitter," Dou.ua, February 6, 2023, https://archive.ph/fOz8J

[136] AJ Vincens, "Hacktivist personas back latest GhostWriter disinfo op targeting Poland, Ukraine," CyberScoop, June 30, 2022, https://cyberscoop.com/ghostwriter-disinformation-russia-belarus-poland-ukraine-refugees/

[137] Джокер ДНР, "Украинские солдатики хвастаются компьютерными программами и смеются над Донецкими из-за использование бумажных карт," Telegram, November 1, 2022, https://t.me/JokerDPR/208 or https://archive.ph/5GjGM

[138] Ibid.

[139] Джокер ДНР, "Продолжаем унижать самоуверенных украинцев программой управления войсками DELTA," Telegram, November 3, 2022, https://t.me/JokerDPR/226 or https://archive.ph/BZQh8

[140] Юрій Бутусов, "Сьогодні російські канали, які контролюються спецслужбами РФ, синхронно оприлюднили інформацію щодо зламу української військової інформаційної системи підтримки рішень та ситуаційної обізнаності Дельта," Facebook, November 1, 2022, https://archive.ph/nmKTB; Євген Пилипенко, "Росія запустила фейк про хакерський злом Delta – унікального бойового софту ЗСУ. Що було насправді," liga.net, November 1, 2022, https://archive.ph/UECQv

[141] Джокер ДНР, "Продолжаем унижать самоуверенных украинцев программой управления войсками DELTA," Telegram, November 3, 2022, https://t.me/JokerDPR/226 or https://archive.ph/BZQh8

[142] On the name change see: Джокер ДНР, "Наши враги заблокировали мой телеграм-канал, но разве можно устранить Джокера?" Telegram, March 25, 2022, https://t.me/s/JokerDPR/1 or https://archive.ph/N3DQg

[143] Some argue that the JokerDNR personality is tied to JokerStash. See: Tanzeel Akhtar, "Darknet's JokerStash Retiring After Making Over $1B Through Illicit Transactions," coindesk, February 12, 2021, https://www.coindesk.com/markets/2021/02/12/darknets-jokerstash-retiring-after-making-over-1b-through-illicit-transactions/;

Serhii Demediuk, former head of the Ukrainian Cyber Police and current Deputy Secretary of the National Security and Defense Council of Ukraine, explained that "a similar example of an information operation aimed at undermining the relations between Ukraine and its neighbors, using social networks, is the dissemination at the end of 2019 through Telegram channels controlled by the special services of the Russian Federation ('Mole of the SBU,' 'Joker DNR') of information about the alleged murder on the border with Hungary, of four SBU officers."[144] Throughout the past years JokerDPR/DNR has been popping up in the context of a variety of Russian information warfare campaigns flagged by Google, Mandiant, Talos, Insikt Group, DFRLab, and others.[145] It is still unknown whether the JokerDPR persona is directly maintained by a Russian intelligence agency or who exactly is managing it. In April 2023, Insikt Group assessed that, "Joker DPR will likely continue to engage in information and propaganda operations that undermine trust in the AFU [Armed Forces of Ukraine] and Ukrainian government, endanger the lives of AFU personnel, and ultimately threaten Ukrainian national security. The potentially far-reaching consequences of Joker DPR's alleged breach of DELTA - specifically, undermining public faith in an asset that has been important to Ukraine's defense - demonstrate that the threat group's activity could affect the outcome of the war in Ukraine."[146]

JokerDPR is not the only adversarial actor that has shown an interest in Delta. Russian cybercriminal groups, such as Void Rabisu, have tried to breach the platform as well. Writing on May 30, 2023, US-Japanese cybersecurity company TrendMicro explained that "because of its many ransomware attacks, Void Rabisu was believed to be financially motivated […]. The motives of Void Rabisu seem to have changed since at least October 2022, when Void Rabisu's associated RomCom backdoor was reported to have been used in attacks against the Ukrainian government and military: In a campaign in December 2022, a fake version of the Ukrainian army's DELTA situational awareness website was used to lure targets into installing the RomCom backdoor. Normally, this kind of brazen attack would be thought to be the work of a nation state-sponsored actor, but in this case, the indicators clearly pointed towards Void Rabisu, and some of the tactics, techniques, and procedures (TTPs) used were typically associated with cybercrime."[147] Speaking to TheRecord in May 2023, Yurii Shchychol, head of the State Service of Special Communications and Information Protection of Ukraine (SSSCIP), equally summarized that, "the Ukrainian military is one of the priorities of Russian hackers. For example, they are constantly trying to attack the Ukrainian battlefield management system Delta."[148]

In May 2024, the SSSCIP published its H2 2023 APT Activity Report #3 which highlighted that "during the second half of 2023, a notable series of attempts to breach national military situational awareness systems utilized by the Security and Defense Forces of Ukraine were observed."[149] The report goes on to note that "a particularly notable case involved a hacker group from the Russian military intelligence agency GRU, which deployed a mobile application mimicking the «DELTA» military app on Google Play before the Ukrainian Ministry of Defense could launch their official version. Russian hackers promoted the download of this deceptive application among Ukrainian military personnel and senior officers."[150]

CyberSec's, "Давайте без имен, немного другая судьба ожидает Джокера, шоп, котрого амеры отлично помнят," Telegram, November 1, 2022, https://t.me/cybersecs/1574 or https://archive.ph/zwqeF

[144] Dmitry Smilyanets, "Ukraine's Top Cyber Cop on Defending Against Disinformation and Russian Hackers," The Record, November 17, 2020, https://therecord.media/ukraines-top-cyber-cop-on-defending-against-disinformation-and-russian-hackers

[145] Shane Huntley, "TAG Bulletin: Q1 2022," February 28, 2022, https://blog.google/threat-analysis-group/tag-bulletin-q1-2022/; Mandiant Intelligence, "Hacktivists Collaborate with GRU-sponsored APT28," September 23, 2022, https://cloud.google.com/blog/topics/threat-intelligence/gru-rise-telegram-minions/; Cisco Talos, "Ukraine Campaign Delivers Defacement and Wipers, in Continued Escalation," January 2, 2022, https://blog.talosintelligence.com/ukraine-campaign-delivers-defacement/; Insekt Group, "Joker DPR and the Information War," Recorded Future, April 6, 2023, https://go.recordedfuture.com/hubfs/reports/cta-2023-0406.pdf; Eto Buziashvili et al., "Russian War Report: Russia and Ukraine warn Zaporizhzhia nuclear plant facing imminent threat," Atlantic Council, August 19, 2022, https://www.atlanticcouncil.org/blogs/new-atlanticist/russian-war-report-russia-and-ukraine-warn-zaporizhzhia-nuclear-plant-facing-imminent-threat/

[146] Insekt Group, "Joker DPR and the Information War," Recorded Future, April 6, 2023, https://go.recordedfuture.com/hubfs/reports/cta-2023-0406.pdf, p. 11

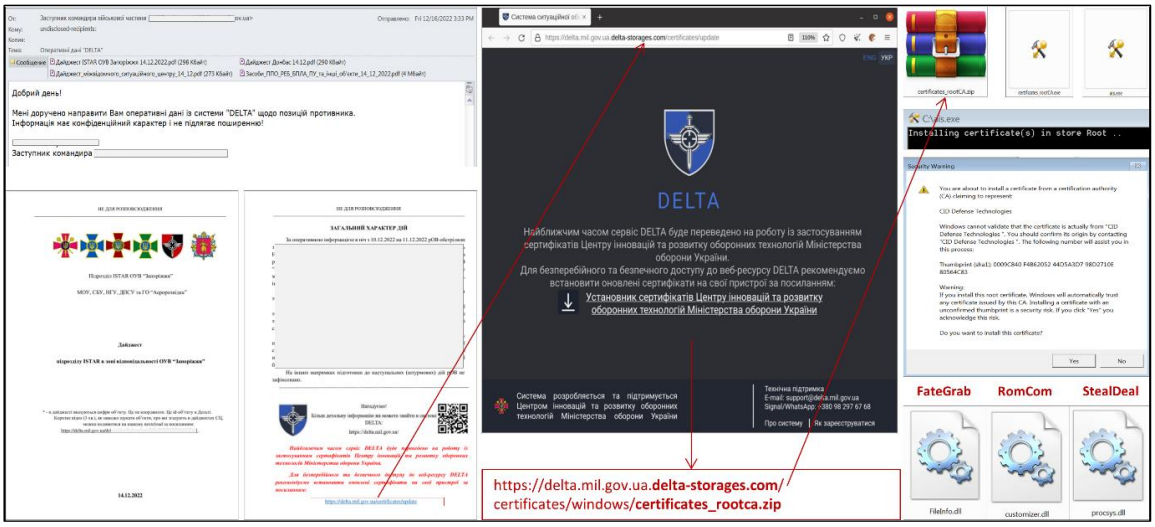
[147] Feike Hacquebord et al. "Void Rabisu's Use of RomCom Backdoor Shows a Growing Shift in Threat Actors' Goals," TrendMicro, May 30, 2023, https://www.trendmicro.com/en_us/research/23/e/void-rabisu-s-use-of-romcom-backdoor-shows-a-growing-shift-in-th.html

[148] Daryna Antoniuk, "Ukraine's cyber chief on the ever-changing digital war with Russia," *The Record*, May 21, 2023, https://therecord.media/ukraine-ssscip-yurii-shchyhol-interview

[149] SSSCIP, "Russian Cyber Operations- APT Activity Report 3 H2 2023," May 3, 2024, https://docs.google.com/viewer?url=https://cip.gov.ua/services/cm/api/attachment/download?id=64622&embedded=true&a=bi, p. 19 or https://archive.ph/jxKHX, p. 19

[150] Ibid., p. 19-20

Figure 30: RomCom/Void Rabisu E-Mail urging users to update their certificates within Delta



Source: CERT-UA, "Кібератака на користувачів системи DELTA з використанням шкідливих програм RomCom/FateGrab/StealDeal (CERT-UA#5709)," December 22, 2022, https://cert.gov.ua/article/3349703

Delta has also been facing its fair share of DDoS attacks. In an interview with Fakty on June 18, 2024, Marat Utyushev, the current head of the Center for Innovation and Development of Defense Technologies claimed that during the last DDoS attack, the system withstood more than 4.5 billion requests.[151] It is unclear whether these metrics are per minute, per second, or a cumulative overall. For context: In its 2023 Q3 report, US DDoS mitigation company Cloudflare highlighted that it mitigated 89 DDoS attacks that "exceeded 100 million requests per second (rps) and with the largest peaking at 201 million rps — a figure three times higher than the previous largest attack on record (71M rps)."[152] In October 2023, Google report that it "mitigated the largest DDoS attack to date, peaking above 398 million rps."[153]

Apart from trying to breach the Delta platform, there have also been information warfare activities to publicly discredit Delta. On the morning of February 24, 2024, Ukrainian news outlet New Voice (NV) published an article stating that "according to our information, a hacker group from Russia penetrated the protected segment of the DELTA system and gained access to databases that stored personal information about civil servants and soldiers of the Armed Forces." The article continued by saying that "Ukrainian authorities are already taking measures to block unauthorized access and protect their nation, but so far the efforts have not been successful. Our sources report the initiation of several criminal cases against high-ranking officials of law enforcement agencies."[154]

One hour later, the article was deleted from the NV website. The news outlet went on to explain that "at 09:28, the website published a news item stating that Russian hackers were allegedly 'tracking the movements of Ukrainian citizens, including law enforcement officers.' Later, it appeared on the NV Telegram channel. The NV editorial team has nothing to do with the posting of this content. The news has now been taken down and the site has been restored. According to NV's sources, the hacker attack was organized to discredit the Delta Armed Forces' situational awareness system."[155]
Aerorozvidka's Twitter account also responded to the incident stating that "we hasten to reassure friends and comrades - today's attack on the website of the NV publication and the information posted there is a hostile [in-

[151] Аеророзвідка, "DELTA – цифрова зброя Сил Оборони України!" Telegram, June 18, 2024, https://t.me/aerorozvidka/1408 or https://archive.ph/0hisi & Факти ICTV, "БОЙОВЕ УПРАВЛІННЯ у СЕРВЕРІ Мережа, яка ОБ'ЄДНУЄ ПІДРОЗДІЛИ Сил оборони," Youtube, June 18, 2024, https://www.youtube.com/watch?v=61vPTrnOM4s, timestamp: 5:00-5:20

[152] Omer Yoachimik & Jorge Pacheco, "DDoS threat report for 2023 Q3," The Cloudflare Blog, October 26, 2023, https://blog.cloudflare.com/ddos-threat-report-2023-q3

[153] Google Cloud, "Google mitigated the largest DDoS attack to date, peaking above 398 million rps," October 10, 2023, https://cloud.google.com/blog/products/identity-security/google-cloud-mitigated-largest-ddos-attack-peaking-above-398-million-rps

[154] Mark Didenko, "Російські Хакери протягом року отримували інформацію про передвіщення громадян України, зокрема співробітників," nv.ua, February 24, 2024, https://web.archive.org/web/20240226151619/https://webcache.googleusercontent.com/search?q=cache:https://nv.ua/ukr/ukraine/politics/rosiyski-hakeri-protyagom-roku-otrimuvali-informaciyu-pro-peredvishchennya-gromadyan-ukrajini-zokrema-spivrobitnikiv-50395657.html

[155] Інна Семенова, "Втручання хакерів у роботу сайту NV: зловмисники розмістили контент, до якого редакція не має стосунку," nv.ua, February 24, 2024, https://nv.ua/ukr/ukraine/events/sayt-nv-bulo-zlamano-24-lyutogo-2024-roku-robotu-vzhe-vidnovleno-novini-ukrajini-50395661.html or https://archive.ph/PHgD5

ternational psychological operation] and another unsuccessful attempt to discredit the key system of situational awareness of DELTA."[156]

* * * *

On February 4, 2023, the Ukrainian Ministry of Defense and the Ministry of Digital Transformation announced that "the government has decided to introduce the Delta system in[to] the Defense Forces. […] In addition to the use of the platform by the military, the government has allowed Delta to be deployed in the cloud outside of Ukraine. This will protect the system from enemy missile and cyber attacks."[157] On January 16, 2024, the Ukrainian Parliament approved document 3549-IX which introduced changes to "improve the processing and use of data in state registers for military accounting and the acquisition of the status of a war veteran during martial law."[158] Among the changes are amendments to Ukraine's law "On Cloud Service" dated February 17, 2022 (No. 2075-IX), concerning "information constituting a state secret using cloud resources and/or data processing centers located abroad."[159] The law now allows that "the processing of such information can be carried out exclusively on the territory of NATO member states on the basis of a joint decision of the Minister of Defense of Ukraine and the General Staff of the Armed Forces of Ukraine […]."[160] Document 3549-IX entered into force on April 2024.[161]

As of this writing, it is unknown whether the Ukrainian government has approached any cloud provider to host the Delta platform outside of Ukraine. Equally, it is unknown how international cloud providers might respond to a request from the Ukrainian government to host Delta on NATO territory. Amazon's AWS for example was the first organization that helped move Ukrainian government data into its cloud environment when Russian tanks were amassing at the Ukrainian border in preparation for the February 2022 invasion.[162] Microsoft equally stepped up during the invasion by moving "16 of the 17 Ukrainian ministries' data to the cloud" onto its servers outside of Ukraine.[163]

That being said, it is unclear whether international cloud providers have a legal obligation to disclose to the governments on whose territory their data centers are physically located on, what military-relevant programs and applications from third countries are hosted in their data centers. Countries who have no such legal obligation in place could potentially become unwitting belligerents in an international armed conflict. And might be subsequently a victim of an armed attack, because of the content hosting decision made by an international cloud provider headquartered somewhere else in the world.

5 Mobile Applications

Several mobile applications feed data and information into the Delta platform as well. Among them are the eEnemy and Stop Russian War Telegram bots and Bachu.

That being said, there are likely other sources that feed data and information into the Delta platform. It could well be that the Prytula Foundation, which in 2022 bought the operating rights of a satellite belonging to Finnish-based SAR satellite imagery provider ICEEYE, feeds data directly into Delta or proxies via Aerorozvidka NGO's situational centers.[164] It could also be that Virazh-Planshet (Віраж-планшет) or Clearview in some way shape or form connect to Delta as well.[165] Given the absence of open-source

---

[156] Aerorozvidka, "Спішимо заспокоїти друзів та побратимів – сьогоднішня атака на сайт видання NV та розміщена там інформація- це ворожа ІПСО та чергова невдала спроба дискредитації ключової системи ситуаційної обізнаності DELTA," X, February 24, 2024, https://twitter.com/aerorozvidka/status/1761458799448133971 or https://archive.ph/8F9Gt

[157] Міністерство оборони України & Міністерство цифрової трансформації України "Уряд ухвалив рішення щодо запровадження системи Delta в Силах оборони," kmu.gov.ua, February 4, 2023, https://web.archive.org/web/20230204190759/https://www.kmu.gov.ua/news/uriad-ukhvalyv-rishennia-shchodo-zaprovadzhennia-systemy-delta-v-sylakh-oborony

[158] Верховна Рада України, "Про внесення змін до деяких законів України щодо удосконалення порядку обробки та використання даних у державних реєстрах для військового обліку та набуття статусу ветерана війни під час дії воєнного стану," zakon.rada.gov.ua, January 16, 2024, https://zakon.rada.gov.ua/laws/show/3549-20#Text or https://archive.ph/3ImdC

[159] Ibid.

[160] Ibid.

[161] Ibid.

[162] Amazon Staff, "Safeguarding Ukraine's data to preserve its present and build its future," June 9, 2022, https://www.aboutamazon.com/news/aws/safeguarding-ukraines-data-to-preserve-its-present-and-build-its-future or https://web.archive.org/web/20240522135645/https://www.aboutamazon.com/news/aws/safeguarding-ukraines-data-to-preserve-its-present-and-build-its-future

[163] Kevin Poireault, "Interview: Microsoft Shares Its Experience of Migrating Data in Times of Cyber Warfare," Infosecurity-magazine, September 30, 2022, https://www.infosecurity-magazine.com/interviews/interview-microsoft-migrating-data/ or https://web.archive.org/web/20240522135653/https://www.infosecurity-magazine.com/interviews/interview-microsoft-migrating-data/

[164] ICEEYE, "ICEYE Signs Contract to Provide Government of Ukraine with Access to Its SAR Satellite Constellation," August 18, 2022, https://www.iceye.com/press/press-releases/iceye-signs-contract-to-provide-government-of-ukraine-with-access-to-its-sar-satellite-constellation; Prytula Fundation, "People's Satellite," n.d., https://prytulafoundation.org/en/about/projects/archive/peoples-satellite

[165] "'Секретная система' помогает ВСУ получать сведения о российских дронах и самолетах," *Focus.ua*, May 31, 2023, https://focus.ua/digital/569874-sekretnaya-sistema-pomogaet-vsu-poluchat-svedeniya-o-rossiyskih-dronah-i-samoletah; Vera

information to confirm these linkages, none of the cases are covered in this report.

5.1 eEnemy (єВорог)

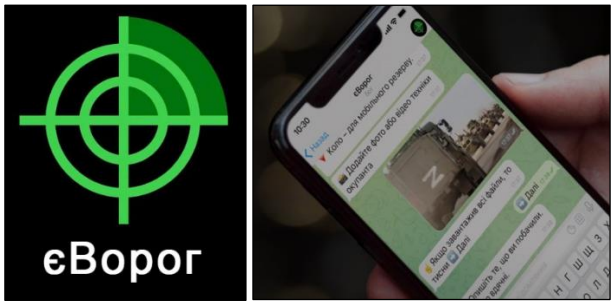
eEnemy (єВорог or eVorog) is a chatbot that was launched by the Ukrainian Ministry of Digital Transformation on March 10, 2022, on the popular messenger app Telegram.[166] The bot allows users to submit photos, videos, and the geolocation of Russian troops, military equipment, explosive devices, and collaborators.[167] Information on Russian troops and military equipment is forwarded to the Headquarters of the Armed Forces of Ukraine. Information on explosives and suspicious devices is shared with the State Emergency Service (SESU).[168] And information on collaborators is directly handed over to the State Security Services (SBU).[169]

To use eEnemy, users have to verify their identity through Ukraine's official Diia e-government application (Дія).[170] Diia was created back in 2020 by the Ministry of Digital Transformation in a push toward a digital Ukrainian state that "helps – not hinders – its citizens."[171] As of this writing, Diia provides Ukrainian citizens access to more than 70+ digital government services, including everything from digitalized driving licenses, COVID certificates, applications for government grants, the recalculation of pensions, marriage applications, and voter registration.[172]

Notably, on June 26, 2024, the US Department of Justice unsealed a grand jury indictment against Russian national Amin Timovich Stigal. The Indictment accuses Stigal of conspiring "with Russian military intelligence on the eve of Russia's unjust and unprovoked invasion of Ukraine to launch cyberattacks targeting the Ukrainian government and later targeting its allies, including the United States."[173] The indictment specifically highlights that Stigal successfully breach the Diia platform on January 13, 2022, and subsequently offered the personal data of 13.5 million Diia users for sale on various dark web forums.[174] Ukrainian parliamentarians seemed to have been surprised by the DoJ's revelations. On July 2, 2024, member of the Ukrainian Parliament Volodymyr Ariev proposed that the Minister for Digital Transformation ought to be invited to a committee meeting to investigate the alleged data leak of 13 million Ukrainians.[175]

eEnemy can be directly accessed via the Diia app, or a user can choose to navigate to the eEnemy bot on Telegram and verify his/her identity with a randomly generated Diia verification link. As the Ukrainian government explains, the verification mechanism was necessary "in order to collect better quality information and to prevent saboteurs from spamming [the bot] with fake photos or videos."[176]

Figure 31-32: eEnemy



Source: Ган Олександра, "«єВорог»: запоріжців просять повідомляти про окупантів через чат-бот," *Gorozhanin*, April 26, 2022, https://gorozhanin.info/ye-vorog-zaporizhcziv-prosyat-povidomlyati-pro-okupantiv-cherez-chatbot/

Once the user's identity has been verified via Diia, the user is asked to specify what object he/she is reporting. Depending on the choice, the eEnemy bot will ask several distinct follow-up questions such as: how many enemy vehicles did you spot; who spotted them (i.e., the origin of the intelligence); the exact time and date the vehicle was

Bergengruen, "Ukraine's 'Secret Weapon' Against Russia Is a Controversial U.S. Tech Company," *Time*, November 14, 2023, https://time.com/6334176/ukraine-clearview-ai-russia/

[166] Міністерство цифрової трансформації України, "Допоможи ЗСУ знищити окупанта: Мінцифра запускає чатбот єВорог," March 10, 2022, https://thedigital.gov.ua/news/dopomozhi-zsu-znishchiti-okupanta-mintsifra-zapuskae-chatbot-evorog

[167] Міністерство цифрової трансформації України, "eVorog — chatbot for civil intelligence in Telegram," May 24, 2022, https://www.youtube.com/watch?v=VTAxA3Omfmw

[168] Міністерство цифрової трансформації України, "Кожне ваше повідомлення про ворожу знахідку в єВорог може врятувати життя," Telegram, November 11, 2022, https://t.me/mintsyfra/3544 or https://archive.ph/UCKCt

[169] Міністерство цифрової трансформації України, "Повідомте про колаборантів на Херсонщині. Корисні чатботи від СБУ та Мінцифри," Telegram, November 16, 2022, https://t.me/mintsyfra/3555 or https://archive.ph/liJ2w

[170] Міністерство цифрової трансформації України, "Допоможи ЗСУ знищити окупанта: Мінцифра запускає чатбот єВорог," March 10, 2022, https://thedigital.gov.ua/news/dopomozhi-zsu-znishchiti-okupanta-mintsifra-zapuskae-chatbot-evorog

[171] Міністерство цифрової трансформації України, "Цифрова держава," n.d., https://plan2.diia.gov.ua/

[172] Міністерство цифрової трансформації України, "Державні послуги онлайн," n.d., https://diia.gov.ua/

[173] US DoJ, "Russian National Charged for Conspiring with Russian Military Intelligence to Destroy Ukrainian Government Computer Systems and Data," June 26, 2024, https://www.justice.gov/opa/pr/russian-national-charged-conspiring-russia-military-intelligence-destroy-ukrainian

[174] US District Court for the District of Maryland, "United States of America v. Amin Stigal," June 25, 2024, https://www.justice.gov/d9/2024-06/amin_stigal_unsealed_indictment_0.pdf, p. 6-7

[175] UNN, "Possible leakage of data from 'Diya': MP proposes to invite Minister Fedorov to a meeting of the relevant committee of the Rada," July 2, 2024, https://unn.ua/en/news/possible-leakage-of-data-from-diya-mp-proposes-to-invite-minister-fedorov-to-a-meeting-of-the-relevant-committee-of-the-rada

[176] Міністерство цифрової трансформації України, "Мінцифри: Побачили окупанта? Повідомте про це в ЗСУ через чатбот єВорог," March 10, 2022, https://www.kmu.gov.ua/news/mincifri-pobachili-okupanta-povidomte-pro-ce-v-zsu-cherez-chatbot-ye-vorog or https://archive.ph/YpJGF

spotted; where it was spotted (the user has to drop a location pin on a digital map); what identifying marks were visible on the vehicle (i.e., the Z, V, and O symbols that identify the different Russian army groups); and it also asks for 3-4 pictures or a 1 minute long video of the spotted vehicle(s).

On October 19, 2022, the Committee on Digital Transformation in Ukrainian Parliament noted on the Parliament's website that "now our defenders need information about: fuel trucks, accumulation and movement of equipment columns, transportation of equipment by rail, warehouses with ammunition, radar stations, artillery positions, field airfields for rotorcraft, the location of the leadership of the enemy forces and the location or residences of the occupiers with geo-positioning. See something from this list and more? Immediately report to the [eEnemy] chatbot from the Ministry of Digital Transformation."[177] On March 22, 2023, the Ministry of Digital Transformation extended that list to include "S300 and Iskander missile systems, [Russian] communication systems, [and] means of electronic warfare."[178]
The information received via eEnemy is checked by one or several intelligence cells. It is unclear whether these cells are military or civilian in nature. According to the Ministry of Digital Transformation, information on Russian troops movements and equipment is then forwarded to the Headquarters of the Armed Forces and entered onto a "digital map."[179] While the Ministry has not specified which digital map this is, the Delta website notes that it integrates the data from "external systems, in particular the chatbots 'eVorog [eEnemy]' and 'Stop Russian War.'"[180] Similarly, Aerorozvidka NGO notes on its website that "one of the most successful achievements of [the] situational centers is the establishment of high-quality interaction between defenders and informers. Ukrainians who are in the occupied territories transmit information on the location and movement of enemy forces using chatbots. The most helpful one is the chatbot of the Ministry of Digital [Transformation], eVorog [eEnemy], which can be accessed from the main screen of the Diia application."[181] As of February 2023, around 462.000 Ukrainians have submitted information via the eEnemy chatbot.[182] And as of January 2023, these included over 7.000 submissions on enemy collaborators.[183]

Ukrainian government officials are fully aware that civilians who use eEnemy might put themselves into extremely dangerous situations. The Ministry of Digital Transformation therefore occasionally reminds users to "not approach enemies and stay at a safe distance from combat. Take photos with a hidden camera so that it is not visible that you have a phone in your hands. Do not post any footage of [the enemy] on social media. Do not discuss enemy movements and enemy vehicle counts over the phone. [And] delete [the] footage from the phone and [all] correspondence from the chatbot, as soon as you [have] inform[ed] the Armed Forces of Ukraine."[184]

From a Ukrainian intelligence gathering perspective, the deployment of eEnemy among the Ukrainian civilian population is an ingenious move. From the perspective of international humanitarian law however, the assessment is a lot murkier. Article 51(3) of the 1977 Additional Protocol I and Article 13(3) of the 1977 Additional Protocol II provide that "civilians shall enjoy protection against the dangers arising from military operations 'unless and for such time as they take a direct part in hostilities.'"[185]
In the context of the war in Ukraine, governments and legal scholar have been rather muted on assessing whether the act of gathering intelligence and digitally submitting information to assist a belligerent, is an act that can be defined as "direct participation in hostilities."
Some military manuals provide clear answers to this question. The US Air Force Commander Handbook of 1980 for example states that "civilians who collect intelligence information, or otherwise act as part of the enemy's military intelligence network, are lawful objects of attack."[186] Similarly, Israel's High Court of Justice stated in 2006 that

[177] Ради України, "Закликаємо повідомляти про окупантів чи колаборантів у чатбот єВорог, - Комітет з питань цифрової трансформації," October 19, 2022, https://www.rada.gov.ua/news/news_kom/229367.html or https://archive.ph/olNan

[178] Міністерство цифрової трансформації України, "Хочете, щоб ворожа техніка палала частіше? Допомагайте Силам оборони інформацією через чатбот єВорог," Telegram, March 22, 2023, https://t.me/mintsyfra/3925 or https://archive.ph/eHMcS

[179] Міністерство цифрової трансформації України, "Одне повідомлення в єВорог може наблизити перемогу. Як обробляють заявки в чатботі," Telegram, February 2, 2023, https://t.me/mintsyfra/3780 or https://archive.ph/FaQbT

[180] Delta, "Delta Wiki - Ключові сервіси," n.d., https://delta.mil.gov.ua/wiki/info/#_2 or https://web.archive.org/web/20230406115016/https://delta.mil.gov.ua/wiki/info/

[181] Aerorozvidka NGO, "Situational awareness is the key to our victory," n.d., https://aerorozvidka.ngo/situational-awareness/ or https://archive.ph/0Vi71

[182] Міністерство цифрової трансформації України, "Як українці допомагали в боротьбі з ворогом," Telegram, February 23, 2023, https://t.me/mintsyfra/3842 or https://archive.ph/jUay8

[183] Міністерство цифрової трансформації України, "Викрили колаборанта – повідомте в чатбот єВорог," Telegram, January 29, 2023, https://t.me/mintsyfra/3763 or https://archive.ph/oCJOq

[184] Міністерство цифрової трансформації України, "Щоб встигнути поласувати кавунами в рідному Херсоні, продовжуймо повідомляти про переміщення та геолокації окупантів і ворожої техніки у чатбот Мінцифри @evorog_bot," Telegram, August 30, 2022, https://t.me/mintsyfra/3368 or https://archive.ph/SxqA5

[185] ICRC, "Practice relating to Rule 6. Civilians' Loss of Protection from Attack," International Humanitarian Law Databases, n.d., https://ihl-databases.icrc.org/en/customary-ihl/v2/rule6

[186] Ibid.

"the following cases should also be included in the definition of taking a 'direct part' in hostilities: a person who collects intelligence on the army, whether on issues regarding the hostilities …, or beyond those issues …; […]"[187]

Military manuals, legal scholars, and policymakers would do well to articulate their legal position on eEnemy for the sake of (1) adapting IHL to the digital realities on the kinetic battlefield, and (2) to provide guidance for their own military personnel to prepare them for the day when they will confront crowdsourcing military intelligence on the future battlefield.
A legal analysis on how and whether the Ukrainian government's implementation of eEnemy – i.e. interfacing with both the official Ukrainian e-government app (Diia) and the country's premier military situational awareness platform (Delta) – is in line with IHL, would be of particular value in the replication debate.

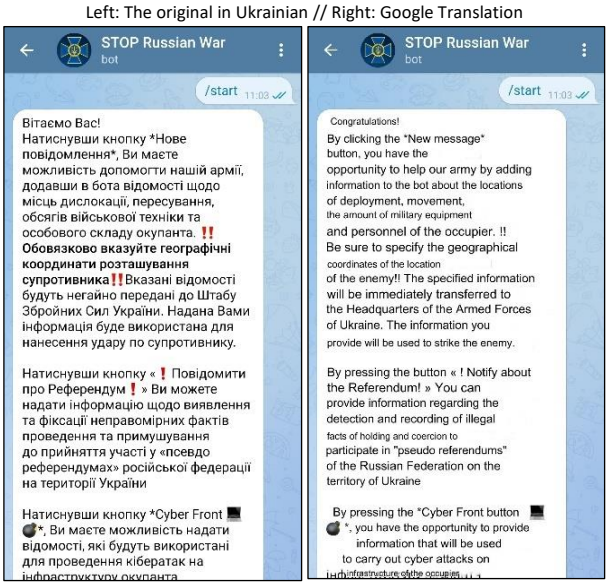
While these legal questions currently remain unresolved, the bottom line is that civilians who use eEnemy could potentially lose their protective status under the Geneva Conventions and become unlawful combatants or even be viewed as spies and be treated as such by the belligerent.[188] Similarly, even civilians who do not use eEnemy and simply take out their phones for other purposes, might – as a consequence of the existence of eEnemy – be mistakenly identified as combatants or spies as well. As of this writing, it is unknown whether any Ukrainian civilians have been shot, imprisoned, or were killed because of their usage (or mistaken usage) of eEnemy.

Behind closed doors, some Ukrainian officials have allegedly tried to minimize the international humanitarian law concerns by highlighting that the information received via eEnemy is actually not militarily relevant for battlefield operations. Their argument is based on the notion that the intelligence cells take way too much time to check the data submitted. Thus, when the data is received by operatives on the front lines, it is largely outdated. If this is true, then the promotion of eEnemy by the Ukrainian government would be particularly heinous and irresponsible, as Kyiv would be willfully putting its own civilians into harm's way without any actual military benefits at all.

5.2 Stop Russian War & Bachu

The SBU maintains its own separate Telegram chat bot called 'Stop Russian War.'[189] Similar to eEnemy, users can submit information on Russian troop movements and military equipment, which is then forwarded to the Headquarters of the Armed Forces of Ukraine.[190] In an interview with My-Ukraina in October 2022, Ilya Vityuk, then head of the SBU's Cyber Security Department, stated that the bot received 100.000 messages on Russian troop movements.[191]

Figure 33: Stop Russian War bot
Left: The original in Ukrainian // Right: Google Translation



Source: Stop Russian War, Telegram, n.d., https://t.me/stop_russian_war_bot

The SBU also asks users to report Russian collaborators, people involved in organizing referenda in the occupied territories, and webcam feeds of Ukrainian roads, industrial facilities, and residential buildings, which could aid the Russian Armed Forces in planning and adjusting their missile strikes and artillery fire in real time.[192]
The Stop Russian War bot is also relevant on the "cyber front." Four days after the Russian invasion, the SBU's Telegram channel explained that they implemented a new function for the bot: "if you possess any information regarding vulnerabilities in Russian cyber defenses (bugs,

[187] Ibid.

[188] Lukasz Olejnik, "Smartphones Blur the Line Between Civilian and Combatant," *Wired*, June 6, 2022, https://www.wired.com/story/smartphones-ukraine-civilian-combatant/

[189] SBU, "Телеграм-бот t.me/stop_russian_war_bot, створений СБУ на початку повномасштабного вторгнення рф, отримав більше 100 тис," Telegram, October 18, 2022, https://t.me/SBUkr/5438 or https://archive.ph/crjaL

[190] National Resistance Center, "Inform the Ukrainian intelligence about the troops of the occupiers," sprotyv.mod.gov.ua, May 1, 2023, https://web.archive.org/web/20230501015002/https://sprotyv.mod.gov.ua/en/transfer-information/

[191] SBU, "Телеграм-бот t.me/stop_russian_war_bot, створений СБУ на початку повномасштабного вторгнення рф, отримав більше 100 тис," Telegram, October 18, 2022, https://t.me/SBUkr/5438 or https://archive.ph/crjaL

[192] SBU, "Цей тиждень став неймовірним," Telegram, September 25, 2022, https://t.me/SBUkr/5188 or https://archive.ph/lZvxJ; National Resistance Center, "Inform the Ukrainian intelligence about the troops of the occupiers," sprotyv.mod.gov.ua, May 1, 2023, https://web.archive.org/web/20230501015002/https://sprotyv.mod.gov.ua/en/transfer-information/; SBU, "СБУ заблокувала вебкамери, які «засвітили» роботу ППО під час ракетної атаки рф на Київ 2 січня," Telegram, January 2, 2024, https://t.me/SBUkr/10757 or https://archive.ph/1j92x

backdoors, credentials), please report it via the chatbot immediately. These may include emails, websites, online-banking, command and control systems, computer networks, certification centers, keys, messengers, social networks, etc. Ukrainian cyber experts will use your information to fight against the occupant!"[193] As of this writing, it is unknown to which unit or department these vulnerabilities are forwarded to, nor how many cyber-relevant messages the SBU actually receives via the bot.

To submit a report to Stop Russian War, user have to provide a valid phone number in case the SBU has additional follow-up questions. This mechanism also serves to dissuade traitors and Russian operatives from submitting false leads. It is unknown whether anyone has ever been intimidated or arrested for submitting a false lead to the Stop Russian War bot. On July 12, 2024, a Russian student in the city of Birobidzhan, located near the Chinese-Russian border was arrested by the FSB for using the Internet and providing information about the location of Russian military units and soldiers in Ukraine to the SBU.[194] While the public coverage of the case is unclear as how the data was transmitted and how the student got in touch with the SBU, one likely vector is the Stop Russian War bot as it does not necessitate Diia verification and is thus open to reports from Russian citizens as well. The student was sentenced to five years in a penal colony for treason.

The SBU also advertises the use of an application called Bachu.[195] Bachu was co-developed by the SBU and a group known as ITStandforUkraine and has a function as eEnemy. Users are asked to submit photos of Russian troop movements, military equipment, aircraft etc. The information submitted to Bachu is likely also forwarded to one or more intelligence cells who feed the data into Delta. There are three names connected to Bachu's development: UA IT Hub, Boco Solutions, and Sergii Tsegelnyk. Sergii Tsegelnyk is the JS Practice Lead in the Kiev office of UK headquartered software company Opinov8. He is also designated as the developer of Bachu on Apple's App Store.[196] Meanwhile, Boco Solutions is designated as the developer of Bachu on Google Play.[197] There is little to no open-source information on Boco Solutions, other than them being likely Ukrainian and having developed a handful of other applications such as Fino – a personal financial assistant.[198] The software development company UA IT Hub (it rebranded to Gart Technology in 2023) is probably the most interesting name connected to the development of Bachu. On their website the company explains their origin story and provides a few more details about Bachu's technical capabilities. The UA IT Hub website notes that "on the 24th of February, with the first air raid siren, civilian Ukrainians were caught with one thought: 'How can I help if I don't have any combat skills?' Techies started to discuss it with their friends and colleagues, and within a few hours, a volunteer community called IT#StandForUkraine was founded. It grew significantly fast, and it happened thanks to word-of-mouth and a solid will to stand for Ukraine's independence. Together we have managed to set up cooperation with other volunteer communities and the government. The volunteer tech movement brought different and unfamiliar people together, and the founders of UA IT Hub learned about the job loss problem from experienced professionals who used to work in prominent Ukrainian outsourced tech companies or promising start-ups and developed products for acknowledged international clients. Now these incredibly talented people help commercial companies to optimize and transform their products or develop new solutions from scratch to achieve your business goals."[199]

The UA IT Hub's website presents Bachu as one of their model case studies. On the development side they explain that "we have integrated a [machine learning] model developed for recognizing and counting military vehicles and Russian soldiers from each users' photos. We have also built a back-end architecture to centralize the data from apps and place the reports on a map."[200] They further state that "users share their coordinates automatically by sending a report via an app, allowing Ukrainian intelligence to place the enemy's forces on a map, validate reports and prevent attacks."[201] Thus, rather than dropping a pin on a digital map, as in the case of eEnemy, Bachu shares the geolocation of the user directly with the SBU.

---

[193] SBU, "ВІДКРИВАЄМО КІБЕРФРОНТ," Telegram, February 28, 2022, https://t.me/SBUkr/3762 or https://archive.ph/HsbUj

[194] Ria Novosti, "В ЕАО студент получил пять лет колонии за сотрудничество с СБУ," July 11, 2024, https://ria.ru/20240711/prigovor-1958875642.html

[195] SBU, "Скільки б росіяни не вдавали, що «феєрверки» на їхніх військових складах і базах стаються через порушення пожежної безпеки, ми знаємо – це кара за їхні злочини в Україні," Telegram, August 17, 2022, https://t.me/SBUkr/4848 or https://archive.ph/2B9cx

[196] App Store, "Bachu," March 18, 2024, https://web.archive.org/web/20240318203557/https://apps.apple.com/ua/app/bachu/id1615836031; Linkedin, "Sergii Tsegelnyk," n.d., https://ua.linkedin.com/in/dr3am3r; Opinov8, "OPINOV8 Statement: We stand with Ukraine," n.d., https://web.archive.org/web/20240531121353/https://opinov8.com/we-stand-with-ukraine/

[197] Google Play, "Bachu," May 2, 2022, https://play.google.com/store/apps/details?id=com.ykotmoar.bachu&hl=en&gl=US&pli=1 or https://archive.ph/bmSGY

[198] APKCombo, "Developer: Boco Solutions," n.d., https://apkcombo.com/developer/Boco%20solutions/ or https://archive.ph/Rqbd1

[199] UAITHub, "About us," March 4, 2023, https://uaithub.com/about-us or https://archive.ph/RvIkv

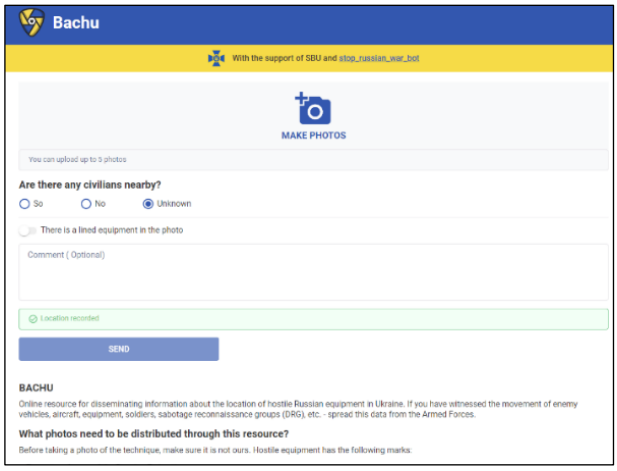
[200] UAITHUB, "Bachu," n.d., https://uaithub.com/case/3; Konstantyn Tupikov, "UA IT Hub – Volunteer Tech Community Turned Developer-First Tech Service Platform," ITKey Media, September 12, 2022, https://itkey.media/ua-it-hub-volunteer-tech-community-turned-developer-first-tech-service-platform/ or https://archive.ph/itu10

[201] Ibid.

What is potentially troubling from an international law perspective, is that Bachu allows users to indicate whether there are any civilians close to the asset they are reporting (see figure 31). Users can choose between three options: "yes," "no," and "unknown." There is no public information available as to what the Ukrainian military does with these user assessments. In a worst-case scenario, a user assessment could serve as the sole military targeting decision. Thus, if a user chooses the "no" option, no further intelligence gathering missions will be conducted and – depending on the significance of the asset(s) identified – the location will be immediately shelled. Conversely, ticking the "yes" or "unknown" option might trigger a drone deployment to surveil the location first. As of this writing, it is unknown why the SBU decided to insert this question into Bachu, and whether the Ukrainian military might be solely relying on the assessment of an unknown civilian to make military targeting decisions for them.

The Bachu application is available for both Apple and Android devices, and it has its own reporting website (bachu.info) through which information can also be sent to the SBU. Users can make 10 reports per day on anything from Russian troops, tanks, aircrafts, Sabotage Assault Reconnaissance Groups (ex., the paramilitary Rusich Group), and broken-down Russian military vehicles. According to the ITStandforUkraine website, Bachu has processed 25.000 reports, its website is visited 40.000 times per day, and it has helped to destroy 2.000 "units of enemy equipment."[202]

Figure 34: Bachu.info (Google Translated)



Source: Bachu.info (geofenced, Ukrainian IP needed)

The SBU and the Ministry of Digital Transformation have also claimed that both Bachu and the Stop Russian War bot have "the ability to transfer information to the Security Service of Ukraine (SBU) without the use of an Internet connection."[203] It is unclear whether this claim is correct in its strictest sense. It might be the case that the Bachu app is able to transmit information via SMS if an internet connection is unavailable. What is more likely however, is that the Bachu app preliminarily stores the outgoing information in the phone's memory and immediately sends it out once an internet connection is available.

According to the privacy policy on the Bachu website [http://bachu[.]info] – which is geofenced and only reachable via a Ukrainian IP address – "sensitive data is stored exclusively in short-term memory for transmission to the internal channels of the State Services, then immediately deleted. Your data is anonymized for transmission. After the transfer, all sensitive data is deleted and we do not store it."[204] Notably, the Bachu website also maintains a section titled: "in case of danger, how to quickly remove the application."[205]

[202] ITStandForUkraine website, Dec. 9, 2022, https://web.archive.org/web/20221209135234/https://www.itstandforua.com/#projects

[203] SBU, "Наш чат-бот http://t.me/stop_russian_war_bot отримав нові можливості! Відтепер надсилати інформацію про пересування ворога можна навіть за відсутності інтернету," Twitter, March 14, 2022, https://twitter.com/ServiceSsu/status/1503410983468941323 or https://archive.ph/jSLA6; StrategEast, "Ukrainian Digital Resistance to Russian Aggression," 2022, https://www.strategeast.org/all_reports/Ukrainian_Digital_Resistance_Report_web.pdf, p. 9

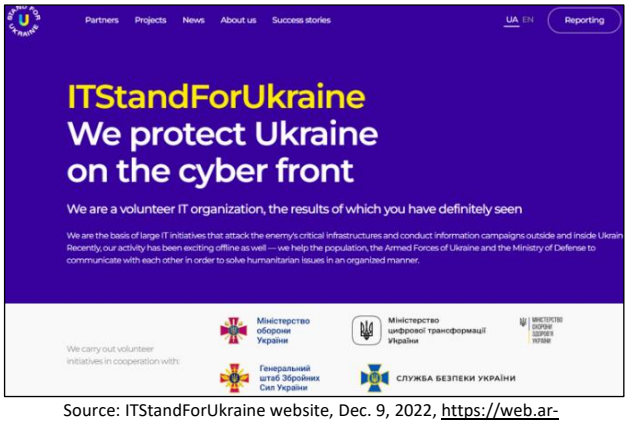
[204] Bachu, "ПОЛІТИКИ КОНФІДЕНЦІЙНОСТІ," n.d., https://bachu.info/privacy or https://archive.ph/OcyeN

[205] Bachu, "В разі небезпеки, як швидко видалити додатокт," n.d., https://bachu.info/security

5.3 ITStandforUkraine

Bachu was in part developed by a volunteer group known as ITStandforUkraine which is headed by Nika Tamayo Flores and Roman Zakharov. The group is unique in the sense that it is deeply entrenched in the Ukrainian IT community. In March 2022, the Associated Press reported that, "Zahkarov ran research at an automation startup" and that ITStandforUkraine is a global movement that includes "software engineers, marketing managers, graphic designers and online ad buyers [in Ukraine and the Ukrainian diasporas abroad]." [206] According to its own website, the group encompasses around 1000+ "'combat' cyber volunteers" that work on more than 40+ active projects in cooperation with the SBU, the MoD, the General Staff of the Armed Forces, the Ministry of Digital Transformation, and the Ministry of Health. According to Zakharov, the group has also conducted several cyber campaigns targeting digital infrastructure in Russia. Speaking to the BBC in April 2023, Zakharov explained that "[the Ukrainian authorities] basically started to give us some target and said what to do when to do [it]."[207] The group targeted "logistics, telecommunication, service companies. There were some disruptions in railway ticketing […] for something like 20 hours."[208]

Figure 35: ITStandForUkraine website (Google Translated)



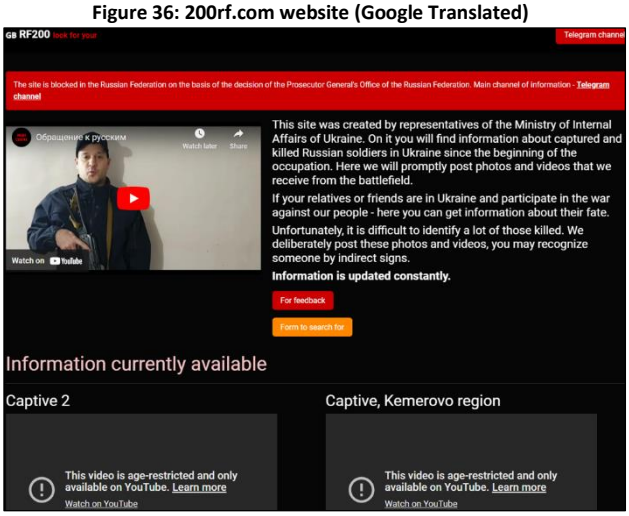
Source: ITStandForUkraine website, Dec. 9, 2022, https://web.archive.org/web/20221209135234/https://www.itstandforua.com/

The BBC interviewed Zakharov in 2023, which was markedly different from Zakharov media interactions the year prior. Dressed now in military fatigue, Zakharov was pointedly asked by the BBC reporter: "You were a big part of and one of the leaders of ITStandforUkraine, what happened, look at you now?" To which Zakharov explained, "I've met a guy who was responsible for the information war. I showed him all the data and all the things that we have been doing. He was amazed and said, 'okay come on … come on Roman … we need it [in the military].' I couldn't resist."[209]

The one project ITStandforUkraine is probably most notorious for is the creation of the 'RF200 Look for Your Own' website (РФ200 Ищи своих) which it developed for the Ukrainian Ministry of the Interior.

The name "RF200" is a combination of the letters RF (РФ) in reference to the Russian Federation, and the number 200 which refers to the military identifier "груз 200" (gruz 200; Engl. Transl.: cargo 200). During the Soviet era, cargo 200 was a well-known term among both Russian and Ukrainian families alike, as these were the Soviet military airlifts that brought the fallen soldiers home from Afghanistan.[210]

Figure 36: 200rf.com website (Google Translated)



Source: 200rf.com, November 2, 2022, https://archive.ph/bcRNo

The RF200 website shows dozens of YouTube-hosted videos of Russian prisoners of war (POW) being interrogated.[211] Back on February 26, 2022, the Ministry of Interior also maintained a 500.00 subscriber strong 'RF200 Look for Your Own' Telegram channel – and several back-up channels.[212] The channels had to move multiple times

[206] Frank Bajak, "Ukraine digital army brews cyberattacks, intel and info-foward," AP, March 5, 2022, https://apnews.com/article/russia-ukraine-technology-europe-software-hacking-da0b91a6502cf7f7ccd7b9481a0074a4

[207] BBC, "How Ukraine and Russia are rewriting the rules of cyber war," Youtube, April 14, 2023, https://www.youtube.com/watch?v=zX9emwKYemE, timestamp: 4:11-4:16

[208] BBC, "How Ukraine and Russia are rewriting the rules of cyber war," Youtube, April 14, 2023, https://www.youtube.com/watch?v=zX9emwKYemE, timestamp: 4:19-4:40

[209] Ibid.

[210] Diana Magnay, "Ukraine invasion: Why the phrase 'Cargo 200' ignites terror among the mothers of Russian soldiers," Sky News, March 1, 2022, https://news.sky.com/story/ukraine-invasion-how-hearing-the-phrase-cargo-200-leaves-relatives-of-russian-soldiers-fighting-in-ukraine-distraught-12554715

[211] РФ200 Ищи своих website, February 27, 2022, https://archive.ph/rXy9L; the videos on the website have not been updated since March 25, 2022. Past videos are still available on the 200rf / Ищи своих (Look For Your Own) Youtube channel: https://www.youtube.com/@user-dp6qh6qt5k/videos

[212] Ищи своих Telegram channel, March 2, 2022, https://web.archive.org/web/20220302072333/https://t.me/rf200_now/; Ищи своих Telegram channel, December 5, 2022, https://web.archive.org/web/20221205003831/https://t.me/rf200_nooow

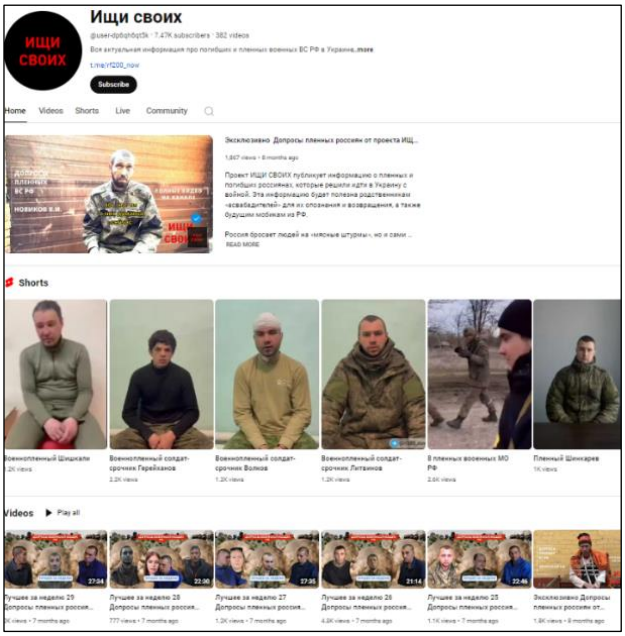
as Telegram has been deleting them due to terms of service violations. Over the course of the war, hundreds of photos and videos of Russian POWs and fatalities – together with their passports and other identifying documents – were published there.[213]

Speaking to CNN, Viktor Andrusiv, the creator and coordinator of the RF200's Look for Your Own Telegram channel and adviser to the Ukrainian Ministry of Internal Affairs, explained that the project was launched to help Russian families track down information about their sons. As Andrusiv put it, "we are not making war against the Russian people. And I don't think they should suffer because of their regime, which lies to them and says everything is good, no one is dying. It's a way for us to bring them some truth."[214]

On March 16, 2022, Human Rights Watch (HRW) published an article titled "Ukraine: Respect the Rights of Prisoners of War - Published Footage of Captured Soldiers Violates Geneva Conventions." In it, HRW called out the Ukrainian Ministry of Internal Affairs and the SBU for posting videos of captured Russian soldiers on Telegram, YouTube, Facebook, and Instagram. HRW notes that the Russian prisoners of war "appear under duress or are revealing their names, identification numbers, and other personal information, including their parents' names and home addresses."[215] It further explains that "the third Geneva Convention and Additional Protocol I address the protection of POWs. They make clear that POWs must be treated humanely in all circumstances and protected against any act of violence, as well as against intimidation, insults, and public curiosity. This includes disclosure of photographs or videos, recordings of interrogations, private conversations or personal correspondence, and any other private data."[216] Rahmin Mahnad, Senior Legal Advisor at the International Committee of the Red Cross (ICRC), similarly noted back in June 2022, that "the prohibition of exposing POWs to public curiosity is driven by two concerns: the desire to preserve the dignity of military personnel who have surrendered or been captured, and the imperative to protect them from harm during their captivity and upon their release."[217] Mahnad goes on to state that, "social media platforms can replicate the transmission of unlawfully disclosed images and information at unprecedented rates, amplifying the vulnerability of POWs to harm, as well as degrading personnel killed in action. The role of content moderators is therefore critical. Images of POWs or fallen combatants, as well as information identifying them, should be systematically removed from social media platforms to the extent feasible."[218]

YouTube has since age-restricted the majority of the 140 individual POW videos that were on rotating display on the rf200 website. Since March 25, 2022, no new videos have been shown on the website. However, as of this writing, YouTube has failed to restrict or delete any of the 382 POW compilation and 26 short videos on the rf200 YouTube channel.[219]

Figure 37: RF200 Look for Your Own Youtube channel



Source: @user-dp6qh6qt5k, "Ищи своих," *Youtube*, May 29, 2024, https://www.youtube.com/@user-dp6qh6qt5k/

Other ITStandForUkraine projects include: Okkupantovnet – which is a website that hosts thousands of Russian mobile phone call recordings intercepted by the SBU and GURMO. And First Aid Bot – which is a Telegram bot that provides first aid recommendations on how to treat critical bleeding, trauma, burns, convulsions, heart attacks, strokes etc. According to ITStandForUkraine, the bot "contains the most important instructions for providing pre-medical care in the conditions of martial law" and is based on order 441, dated March 9, 2022, by the Ministry of Health of Ukraine.[220] The bot also highlights that, "the

[213] Ищи своих Telegram channel, December5, 2022, https://web.archive.org/web/20221205003831/https://t.me/rf200_noooow

[214] Eliza Mackintosh, "The bodies of Russian soldiers are piling up in Ukraine, as Kremlin conceals true toll of war," CNN, March 23, 2022, https://edition.cnn.com/2022/03/23/europe/ukraine-war-russian-soldiers-deaths-cmd-intl/index.html

[215] HRW, "Ukraine: Respect the Rights of Prisoners of War: Published Footage of Captured Soldiers Violates Geneva Conventions," March 16, 2022, https://www.hrw.org/news/2022/03/16/ukraine-respect-rights-prisoners-war

[216] Ibid.

[217] Ramin Mahnad, "Shielding prisoners of war from public curiosity," ICRC, Humanitarin Law & Policy, June 28, 2022, https://blogs.icrc.org/law-and-policy/2022/06/28/shielding-prisoners-of-war-from-public-curiosity/

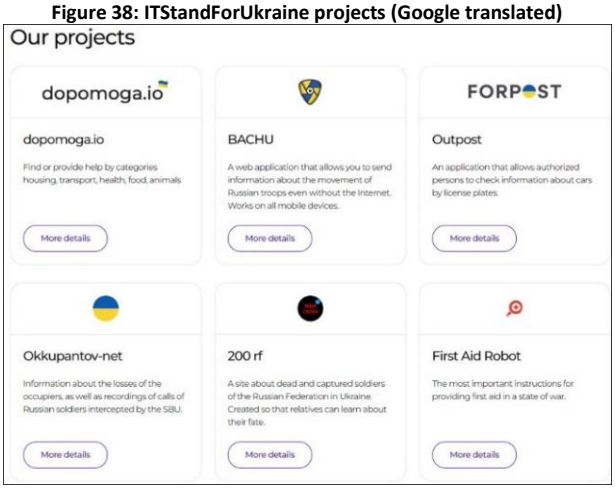
[218] Ibid.

[219] @user-dp6qh6qt5k, "Ищи своих," Youtube, n.d., https://www.youtube.com/@user-dp6qh6qt5k/videos

[220] ITStandForUkraine website, Dec. 9, 2022, https://web.archive.org/web/20221209135234/https://www.itstandforua.com/#projects under First Aid Robot – more details

user of the bot bears all risks on its own. In case of emergency, immediately call the emergency service."[221]

Figure 38: ITStandForUkraine projects (Google translated)



Source: ITStandForUkraine website, Dec. 9, 2022, https://web.archive.org/web/20221209135234/https://www.itstandforua.com/#projects

5.4 ePPO (єППО)

ePPO (єППО or єдиної протиповітряної оборони; Engl. Transl.: United Air Defense Complex) is a mobile phonse application that was developed by the Ukrainian volunteer group Technary. Technary was founded by Gennadiy Suldin, Andriy Kosyak, and Igor Astakhov. Currently, the group has around 10 people working on several different projects, including Chaika (an electronic simulator designed for training night anti-aircraft firing), and Poloz (a laser-thermal imaging station to illuminate aerial targets).[222] In October 2022, Astakhov explained to dev.ua that, "I, along with Gennadiy Suldin and Andriy Kosiak, started cooperating with the [military] headquarters long before the full-scale war in Ukraine. [In 2022], Gennady and Andriy were the only civilians at the air defense conference. Representatives of various branches of the military were present there, and various proposals for improving the effectiveness of air defense systems were presented. At this conference, various improvements were discussed, and Gennady and Andriy presented the development of a modern solution [ePPO] for tracking cruise missiles, which will make it possible to eliminate them 100%."[223]

ePPO is the only mobile application – known to this author – that has been approved by Ukraine's military intelligence service (GURMO). In fact, according to ePPO's website, "the development of the application was accompanied from the very beginning by the Ukrainian military – they suggested, criticized, supplemented, and supported" the app.[224]

Figure 39: ePPO website (Google translated)

Source: Eppo website, May 29, 2024, https://web.archive.org/web/20240529122348/https://eppoua.com/

EPPO is designed to help the Ukrainian military widen its real-time human intelligence network to defend against incoming Russian air breathing threats – particularly low-flying assets that evade Ukrainian radar detection. This encompasses information on the location and flightpath of Russian fighter jets, helicopters, drones, cruise missiles, but also the occurrence of explosions. As the ePPO websites explains, "fishermen on rivers, truck drivers, and even your grandmother just digging potatoes - they can all help save lives. It is these people who can see objects that fly outside the coverage of military radars and which the enemies deliberately hide."[225] According to ePPO's official Telegram channel, more than 528.000 Ukrainian citizens have downloaded the ePPO application since March 11, 2024.[226]

The way ePPO works is fairly straightforward. Users download the application onto their smartphone from either the Apple App Store or Google Play. They then verify their identity via the Diia application.[227] As with all mobile applications that use Diia as identity verification method, the Ukrainian government can access a user's personal in-

[221] @FirstAidRobot, "Перша домедична допомога FirstAidRobot," Telegram, n.d., https://t.me/FirstAidRobot

[222] Technary, "Software and Hardware for Air Defense Forces," May 31, 2024, https://www.technary.com.ua/en/#projects or https://archive.ph/kssgI

[223] Марія Бровінська, "«єППО» вперше допоміг збити російський «Калібр». Як розроблений українцями застосунок оберігає від ворожих ракет: інтерв'ю з розробником," dev.ua, October 26, 2022, https://dev.ua/news/ieppo-1666267811 or https://archive.ph/nLxlj

[224] EPPO website, http://www.eppoua.com, under "Чому саме єППО?"

[225] EPPO website, http://www.eppoua.com, under "Чому саме єППО?"

[226] EPPO, "Групі Технарі 2 роки. Звіт про наші розробки для протиповітряної оборони та їх впровадження в ЗСУ," Telegram, March 11, 2024, https://t.me/eppo_official/1597 or https://archive.ph/rHlaM

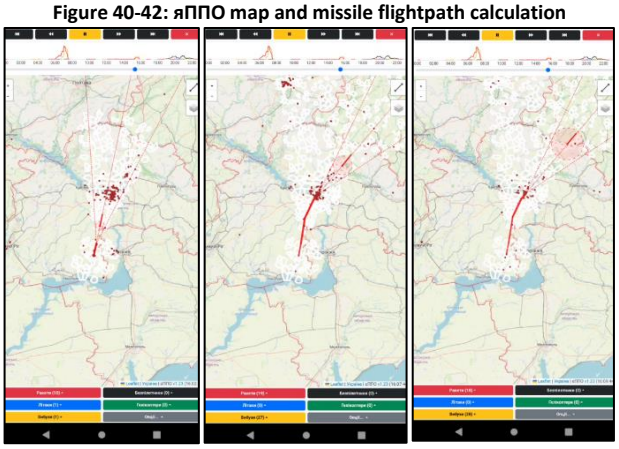
[227] EPPO, "Повідомити про окупантів, допомогти ППО та знайти безпечне місце Корисні сервіси у воєнний час," Telegram, October 18, 2023, https://t.me/eppo_official/1269 or https://archive.ph/j5Y1z; EPPO, "Ми часто отримуємо запитання про те," Telegram, January 3, 2024, https://t.me/eppo_official/1424 or https://archive.ph/Oxoj6

formation if the user sends in multiple false ePPO reports.[228] In the ePPO application users have to then chose the air asset they want to report, point the arrow on the top of the screen toward the asset's location or flightpath, and then press the big red button to send the information to the armed forces.[229]

In its instructions, ePPO emphasizes that "your safety is above all else! Before using [ePPO], you have to make sure that you are in a safe place. You don't need to photograph anything. No need to record video or audio. If you are not sure where the object is flying, you can not use the arrow. Your geolocation will be enough. The data from your device's compass is auxiliary. If you're not sure if your device's compass is working correctly, or if you're unsure of the exact flight direction of your target, don't worry. Send a message anyway!"[230]
According to a news item published by GURMO, the information that users report via ePPO will be seen by "air defense specialists"" who will "see a mark on a map" that will "complement the radar information and the [air threat] will be shot down."[231]

Overall, ePPO consists of three parts: (1) the ePPO mobile application; (2) a server platform on the back-end called яППО, which displays all reports submitted via the ePPO application on a digital map and calculates the most probable flightpaths of the incoming air threat.[232] According to the ePPO Telegram channel, more than 1.000 air defense personnel have dedicated accounts on the server to access the map and flightpath predictions;[233] and (3) a military communication system called яППО Стрілець (Engl. Transl.: Sagittarius air defense system), that allows the military headquarter to transmit shoot down orders to all the air defense units along the air threat's flightpath.[234] For this to function effectively, the headquarter must continuously update the movement of every Ukrainian air defense unit in the яППО Стрілець system. According to Astakhov, Technary has made яППО Стрілець available only to the Ukrainian military.[235] No other Ukrainian entity has access to it.

Figure 40-42: яППО map and missile flightpath calculation



Source: ePPO Telegram channel, "On January 23, 2024, the enemy attacked the city of Dnipro with a missile. The air defense system received the first alerts from citizens at 16:00. At 16:01, the target's motion vector was built, which led to an instant reaction of the "It's flying at you" system, which notified the residents of Dnipro about the danger. At 16:05, the missile was already over the city. According to notifications from the Vostok PMC, it became known that the missile had been eliminated," January 24, 2024, https://t.me/eppo_official/1456 or https://archive.ph/xEAaA

It is unknown whether the information submitted via the ePPO application is also shared with other digital platforms or mobile applications. It could well be that Aerorozvidka NGO's situational centers have access to ePPO or яППО. Some information might also be flowing into Delta. While it is not known whether ePPO interfaces with Air Alarm and other Ukrainian mobile applications that warn Ukrainian citizens of incoming air strikes, Technary did implement its own air strike warning notifications for all ePPO users called В Тебе Летить (Engl. Transl.: It's coming at you).[236] In a posting on Facebook on July 2023, Gennadiy Suldin, one of the ePPO developers, explained that "from today, users of the eppo application will also be able to receive personalized warnings about an air threat just for them, when their coordinates are close to the calculated flight path of Russian scrap metal in 5-10 minutes. The great "accuracy" of swamp missiles that can come anywhere, and debris from the sky during air combat will no longer be a bloody surprise, because after a personal

[228] EPPO website, May 31, 2024, http://www.eppoua.com or https://archive.ph/vkhfD

[229] EPPO website, http://www.eppoua.com, under "Як встановити єППО"

[230] EPPO website, http://www.eppoua.com, under "Як користуватися єППО"

[231] Головного управління розвідки Міністерства оборони України, "Українці через застосунок єППО можуть допомогти зенітникам збивати ворожі дрони та ракети," gur.gov.ua, October 13, 2022, https://gur.gov.ua/content/ukraintsi-cherez-zastosunok-ieppo-mozhut-dopomohty-zenitnykam-zbyvaty-vorozhi-drony-ta-rakety.html or https://archive.ph/cPkEp

[232] Марія Бровінська, "«єППО» вперше допоміг збити російський «Калібр». Як розроблений українцями застосунок оберігає від ворожих ракет: інтерв'ю з розробником," dev.ua, October 26, 2022, https://dev.ua/news/ieppo-1666267811 or https://archive.ph/nLxlj

[233] EPPO, "Групі Технарі 2 роки. Звіт про наші розробки для протиповітряної оборони та їх впровадження в ЗСУ," Telegram, March 11, 2024, https://t.me/eppo_official/1597 or https://archive.ph/rHIaM

[234] Марія Бровінська, "«єППО» вперше допоміг збити російський «Калібр». Як розроблений українцями застосунок оберігає від ворожих ракет: інтерв'ю з розробником," dev.ua, October 26, 2022, https://dev.ua/news/ieppo-1666267811 or https://archive.ph/nLxlj

[235] Ibid.

[236] Ajax, "The Air Alert app is now available for Android and iOS," n.d., https://ajax.systems/blog/zastosunok-povitryana-trivoga/ or https://archive.ph/ilmMe; Rīta Panorāma, "Smiltēns: Kyiv could help Rīga with civil defense expertise," *eng.lsm.lv*, January 24, 2023, https://eng.lsm.lv/article/society/defense/smiltens-kyiv-could-help-riga-with-civil-defense-expertise.a493035/ or https://archive.ph/J31cY

warning, eppo users and their loved ones will have at least a few minutes to hide from the windows."[237]
EPPO's public comments seem to imply that the яППО server is solely administered by Technary. It is unclear whether Technari has an agreement with the Ukrainian Armed Forces or the intelligence services to protect яППО from cyber threats.

Overall, ePPO's setup is battletested and able to significantly reduce the detection times for incoming air breathing threats. In terms of metrics, information received via ePPO is transmitted to the military within five seconds.[238] It has also provided the armed forces with a faster sensor-to-shooter loop to intercept air threats more efficiently. Talking to The Guardian in October 2022, Suldin noted that the aim of ePPO is to "enlist 'the entire population' in helping to spot incoming attacks in what he described as an example of 'web-centric war.'"[239] Speaking at the Ukraine Media Center in October 2022, Suldin noted that "representatives of the air defense forces of some NATO countries wrote to us, they asked us a few interesting questions, we answered, but I cannot tell you about this in detail."[240]
The ePPO website mentions an additional company that is involved in the development of ePPO: Mate and Mate. Mate and Mate is a London-based creative agency founded in 2016. The company specializes in advertisement, analytics, user interface design, and web and mobile engineering. For ePPO it designed the app's user interface and website. Mate and Mate's staff primarily consists of ethnic Ukrainians. Among its clients are major companies such as Coca-Cola, Adidas, and P&G. Notably, on its website, but without any specific date, Mate and Mate lists an ePPO statistics: 900.000+ reports were submitted via the ePPO app, approximately 85% of reported air threats were destroyed, and that ePPO can track up to 290 targets simultaneously.[241]

ePPO's usefulness on the battlefield has been recognized in Russia. In mid-August 2023, the All-Russia Popular Front coalition (Общероссийский народный фронт) released an application called Радар.НФ (Engl. Transl.: Radar.NF – NF is the abbreviation for the Popular Front).[242] According to Vladimir Taranenko, head of the Popular Front's youth wing, the idea for developing the app originated with members of the Cyber Squad (Кибердружины). The Cyber Squad is state-supported Russian volunteer association whose members are tasked to purge the web of "illegal" information, i.e., information that promotes war, incites national, racial, or religious hatred and enmity in or against Russia.[243]

The application was then developed under the auspices of the Popular Front in cooperation with the Russian Ministry of Defense. As Mikhail Kuznetsov, head of the Popular Front's executive committee emphasized, "thank you very much to our Ministry of Defense, our military. The fact that our colleagues met our needs and that they responded and reacted and agreed to build such joint work is very worthwhile. This once again confirms the most important thesis that 'the people and the army are united.'"[244]

Figure 43: Radar.NF online advertisement

Source: Народный фронт, "ATACMS, HARM, 'Ольха' сегодня ночью атаковали Крым, Белгородскую, Курскую и Брянскую области," Telegram, May 15, 2024, https://t.me/onf_front/10985 or https://archive.md/7VeB8

Radar.NF looks and functions very similar to ePPO. Even the official ePPO Telegram account noted that "Russian's learned about eppo. Russians shat on eppo. Russians rec-

[237] Gennadiy Suldin, "Жахлива статистика. Велика кількість українців під час російських повітряних атак травмовано чи вбито уламками скла," *Facebook*, July 21, 2023, https://archive.ph/jiaBb

[238] EPPO, "Натрапили у Twitter. Хочемо прокоментувати," July 19, 2024, https://t.me/eppo_official/1786 or https://archive.is/etfoK

[239] Dan Sabbagh, "Ukrainians use phone app to spot deadly Russian drone attacks," *The Guardian*, October 29, 2022, https://www.theguardian.com/world/2022/oct/29/ukraine-phone-app-russia-drone-attacks-eppo

[240] Ukraine Media Center, "SOME NATO REPRESENTATIVES SHOWN INTEREST IN THE UKRAINIAN-MADE 'EPPO' APP," October 27, 2022, https://web.archive.org/web/20230228161813/https://mediacenter.org.ua/strong-some-nato-representatives-shown-interest-in-the-ukrainian-made-eppo-app-strong/

[241] Mateandmate," Unified Air Defense Complex," n.d., https://web.archive.org/web/20240529132904/https://mateandmate.com/work/eppo

[242] народный фронт, "РАДАР.НФ," August 18, 2023, https://onf.ru/radar or https://archive.ph/AwbPw

[243] Cybersquad, "Центр информационной безопасности и психологической помощи молодежи Ханты-Мансийского автономного округа Югры," n.d., https://cybersquad.ru/ or https://archive.ph/jwmwx; BBC, "Кибердружины от "Единой России" будут искать в интернете нелегальный контент," November 2, 2018, https://www.bbc.com/russian/news-46074279 or https://archive.ph/m5yqB

[244] Мария Материкова, "Кибердружина Народного фронта разработала мобильное приложение для сигналов о беспилотниках и ЧС," August 17, 2023, https://pravda-nn.ru/news/kiberdruzhina-narodnogo-fronta-razrabotala-mobilnoe-prilozhenie-dlya-signalov-o-bespilotnikah-i-chs/ or https://archive.ph/Ug3AP

ognized eppo. Russians attacked eppo. Russians plagiarized eppo. Then comes the stage when everything stolen from us is scaled in the Russian Federation faster than us. So install Ukrainian eppo and become part of the country's defense."[245]

Radar.NF has been promoted across Russia's western front, from a kindergarten in Crimea to the city administration of Murmansk in Russia's high north.[246] Vyacheslav Gladkov, governor of the front-line region of Belgorod, explained on Telegram that "our region has been subjected to constant shelling by the Ukrainian armed forces since the first days of the special military operation. There have been many incidents, including those involving unmanned aerial vehicles. A lot of questions have always come in about where to call to pass on this or that information. To date, we have said that it is necessary to call 122 or contact, for example, police officers, the duty services. This efficiency has not always satisfied you, dear friends. Today, the Popular Front has developed an application for smartphones called Radar. This application allows you to transfer operational information to law enforcement agencies to analyze and quickly make a decision."[247]

Android users can download the application on Google Play, while Huawei smartphone users can get it from RuStore. As of this writing, the application has more than 100.000 downloads on each platform.[248] According to Pravda-nn.ru, Apple refused to host the application in its App Store due to U.S. sanctions.[249]

In terms of metrics, the Telegram channel of the Popular Front provides some insights. On April 27, 2024, the channel summarized that "that night 33 signals were received, 12 of them were about UAVs. And they helped! They were submitted in the application [Radar.NF], and thanks to this, among other things, 66 drones were destroyed by Russian air defense forces. And this is only the Krasnodar region. And this is only in a few hours."[250] On March 13, 2024, "17 signals from civilians were received by the Popular Front app 'RADAR.NF' for this night and morning. Reactions came from the Belgorod region, Voronezh region and Lipetsk. In total, air defense systems destroyed 58 Ukrainian drones on Russian territory, the Ministry of Defense reports. Thank you, people. Your signals helped to notice enemy drones in time. Together we let's do more!"[251]

By comparison, on May 26, 2024, the ePPO telegram channel reported that, "during the night, the enemy launched a powerful attack on Ukraine, using 31 Shahed, 12 cruise missiles and 2 Kinzhal missiles. It was a difficult night, but thanks to our indomitable air defense monitors, we were able to alert thousands of people to the danger. More than 1700 observers reported seeing dangerous objects overhead. […] Thanks to these efforts, about 34 thousand people received timely warnings through the 'It's coming at you' system."[252]

6 Terminal (Термінал)

Delta was not the only situational awareness platform that was deployed in the defense of Kyiv in March 2022, nor was Aerorozvidka the only group manufacturing drones in Ukraine. An information and telecommunications system named Terminal was developed by Kyiv-based defense innovation company UkrSpecSystems. UkrSpecSystems is probably most famous for the manufacturing of the People's Drones, i.e., the PD-1 and PD-2 multipurpose unmanned aerial vehicles (UAVs).

The origin story of UkrSpecSystems is similar to that of many other Ukrainian defense start-ups. UkrSpecSystems explains on its website that, "we founded our company back in 2014 at the very beginning of the Russian intervention in Eastern Ukraine. At that time, the Ukrainian army had zero drones that were ready for full-scale war deployment. Drones manufactured by foreign companies

---

[245] EPPO, "Стадии принятия неизбежного в РФ на примере украинской разработки еппо," Telegram, August 17, 2023, https://t.me/eppo_official/1035 or https://archive.ph/FrFGl

[246] Детский сад № 11 Сказка, "Приложение Радар.НФ," November 21, 2023, https://feodou11.crimea-school.ru/content/prilozhenie-radarnf or https://archive.ph/QxXXT; Официальный сайт администрации города Мурманска, "Народный фронт запустил мобильное приложение Радар. НФ," September 19 2023, https://www.citymurmansk.ru/novosti/?newsid=25732 or https://archive.ph/oDiNk

[247] Настоящий Гладков, "Наша область с первых дней специальной военной операции подвергается постоянным обстрелам со стороны ВСУ," Telegram, August 17, 2023, https://t.me/vvgladkov/3339 or https://archive.ph/Esb3Z

[248] Общероссийский народный фронт, "Радар.НФ," Google Play, May 20, 2024, https://play.google.com/store/apps/details?id=ru.onf.rdr&hl=en&gl=US or https://archive.ph/wOlB9; Народный фронт, "Радар.НФ," RuStore, March 20, 2024, https://www.rustore.ru/catalog/app/ru.onf.rdr or https://archive.ph/zWkEe

[249] Мария Материкова, "Кибердружина Народного фронта разработала мобильное приложение для сигналов о беспилотниках и ЧС," August 17, 2023, https://pravda-nn.ru/news/kiberdruzhina-narodnogo-fronta-razrabotala-mobilnoe-prilozhenie-dlya-signalov-o-bespilotnikah-i-chs/ or https://archive.ph/Ug3AP

[250] Народный фронт, "В эту ночь поступило 33 сигнала, 12 из них были о БПЛА," Telegram, April 27, 2024, https://t.me/onf_front/10921 or https://archive.ph/5vRpP

[251] Народный фронт, "17 сигналов от мирных жителей поступило в приложение Народного фронта "РАДАР.НФ" за эту ночь и утро," Telegram, March 13, 2024, https://t.me/onf_front/10618 or https://archive.ph/KVANd

[252] EPPO, "Вночі ворог завдав потужного удару по Україні," Telegram, May 26, 2024, https://t.me/eppo_official/1712 or https://archive.ph/FhU1u

were excessively expensive ($500 000 and higher). Moreover, it was technically impossible to import them to Ukraine due to complex custom restrictions. As soon as we realized this problem, we immediately began our own drone production."[253] Speaking to Ukrainian defense outlet OPK in March 2020, UkrSpecSystem's commercial director Yuriy Kiskin further explained that "we gathered a group of enthusiasts and made the first, as they say, folk drone. Hence the name People's drone (PD-1). Accordingly, the first samples were transferred to the Armed Forces free of charge, and our servicemen used them in the combat zone. Over time, UAVs began to improve, and the idea came from military operators that if UAVs were manufactured by some enterprise, then perhaps the army would consider acquiring them."[254]

On the Terminal system, Kiskin notes that "today, the process of not just flying with the aim of obtaining photos/videos, but having an integrated system, is coming to the fore all over the world. We are in favor of an integrated system that will allow us to perform the tasks that the military personnel face as efficiently as possible. For this we have [the] software, [T]erminal. This allows you to plot objects on the map online, in real piloting mode, process these objects, and transfer them promptly to users. Starting from a soldier with a tablet and ending with the headquarters of the command in the General Staff, who will see the operational situation online with all the marks in their headquarters. We are moving towards the software part in parallel with the hardware. If we talk about product development, then we see the UAV not only as an aircraft that flies, shooting a video or photo. This is a complex."[255]

Terminal is quite an interesting platform for which very little open-source information is available. A 2018 UkrSpecSystem's product brochure merely states that the 'Terminal 2.0 Software' can "receive video feeds from stationary cameras, drones and other sources of visual information in one software; see all sources of visual feed on map; control your sources of visual information; create object and targets on map; add augmented reality to real-time video feed; plan your intelligence missions; detect, identify and analyze targets; record important events; quickly analyze aerial video and photo information; create reports based on received information; log all changes."[256]

More detailed insights into the system were made available in September 2022, when Mykhailo Rakushev, from the National Defense University of Ukraine, together with Vitaly Zuyko and Roman Pantyushenko, from the Central Research Institute of the Armed Forces of Ukraine, published a journal article titled "Analysis of the use of the 'Terminal' Information and Telecommunication System in the Interests of the Defense Forces of Kyiv."[257] In the article, Rakushev et al. explain how the Terminal system works, how it was used during the defense of Kyiv in March 2022, and how it fits in relation to Delta.
Rakushev et al. estimate that more than 600 UAVs were involved in the defense of Kyiv in March 2022.[258] More than 300 of these were distributed to the Ukrainian Armed Forces by volunteer networks. Because of the numerous different types of UAVs involved, it "turned out to be impossible to organize the collection, processing, exchange and display of information received from UAVs with standard software and technical means – due to their banal absence."[259] The deployment of Terminal and Delta subsequently filled this gap in different ways.

Terminal consists of five elements: (1) The Terminal software suite, (2) a local cloud server, (3) a main remote cloud server, (4) multiple user workstations, and (5) communication channels. The Terminal software suit is deployed on a local server that does all the heavy computational lifting. It comes pre-loaded with 600 GBs of electronic maps (such as Google Hybrid, Google Earth, OpenStreetMap) and an integrated database of Russian military equipment. The local server receives all the intelligence that is submitted by stationary and mobile cameras, UAVs, and also intakes spatial imagery. Users connect to the server via a virtual private network (VPN) based on the OpenVPN protocol. Rakushev et al. note that "experience has shown that household personal computers and laptops, including those purchased commercially by volunteers, were widely used to deploy workplaces."[260] VPN keys were generated and issued to a user once their identity has been verified by their respective military unit. Rakushev et al. state that "until June 2022,

[253] Ukrspecsystems, "Company's history," n.d., https://ukrspecsystems.com/about or https://web.archive.org/web/20240522140037/https://ukrspecsystems.com/about

[254] Дмитрий Бадрак, "БЕСПИЛОТНЫЙ ВЗЛЕТ КОМПАНИИ «УКРСПЕЦСИСТЕМС»: ОТ ВОЛОНТЕРОВ ДО ЛИДЕРОВ НА РЫНКЕ. Часть 1," *OPK*, March 10, 2020, https://opk.com.ua/беспилотный-взлет-компании-укрспец or https://web.archive.org/web/20240522140110/https://opk.com.ua/беспилотный-взлет-компании-укрспец

[255] ibid.

[256] Ukrspecsystems, "Презентация и брошюра компании «Ukrspecsystems»," February 23, 2018, https://web.archive.org/web/20240522140655/https://www.slideshare.net/slideshow/ukrspecsystems/88730862

[257] Ракушев et al. "Аналіз використання інформаційно-телекомунікаційної системи "Термінал" в інтересах сил оборони Києва," Modern Information Technologies in the Sphere of Security and Defense, Volume 44, No. 2, September 2022, http://sit.nuou.org.ua/article/view/264158/261332

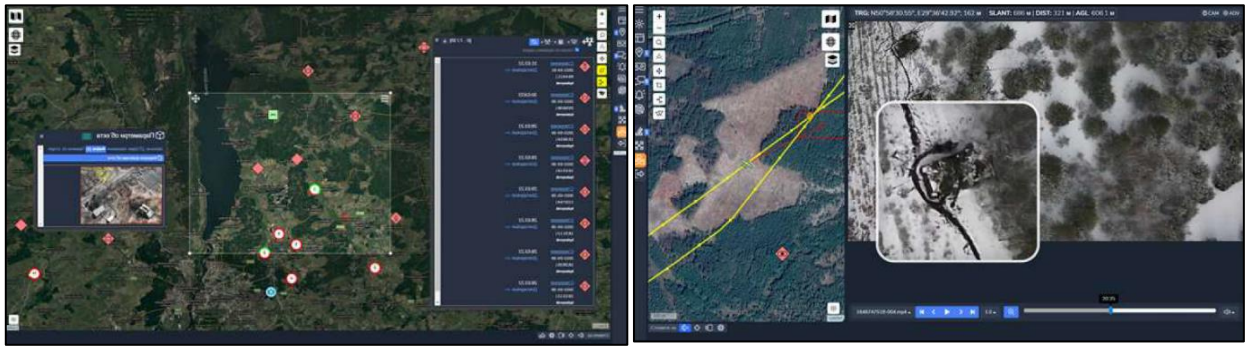
[258] Ibid., p. 58

[259] Ibid., p. 54

[260] Ibid., p. 57

the [Terminal] developer[s] used a commercial cloud service to obtain VPN keys. After June 2022, the developer operated its own cloud VPN server."[261]

Figure 44-45: (left) Staff/Headquarter mode; (right) Decryptor mode



Source: Rakuchev et al. "Аналіз використання інформаційно-телекомунікаційної системи "Термінал" в інтересах сил оборони Києва," Modern Information Technologies in the Sphere of Security and Defense, Volume 44, No. 2, p. 56

The Terminal software suite encompasses five operating modes: (1) administrator mode, (2) staff/headquarter mode, (3) decryptor mode, (4) "observer-adjuster of the stationary video camera system" mode, and (5) "reconnaissance-corrector with UAV" mode. The administrator mode is for adding new users, managing access permissions, and system security. The staff mode opens a digital map and allows users to view and generate analytical reports on user added objects, as well as adding your own objects and intelligence onto the map. The decryptor mode was probably the most impactful functionality during the defense of Kyiv as it enables easy data intake and the processing of video, photo, and log files from a multitude of different UAV systems. The observer adjusted mode is for "monitoring the situation using cameras, controlling the direction of observation, determining the coordinates of objects using coupled observation and performing informational analysis."[262] And the reconnaissance-corrector mode allows for the control a UAVs payload and to target an enemy asset in real time. Rakushev et al. however note that this mode "functions only for UAVs produced by UkrSpecSystems."[263]

The arrival of hundreds of Starlink terminals in Kyiv on February 28, allowed the Kyiv Defense Forces to extend their surveillance operations into areas outside the city that lost cell and internet coverage.[264] Starlink also enabled local servers to maintain stable internet connectivity and allowed for high-speed data exchange, which in turn enabled the vast deployment of Terminal and Delta on the battlefield.

Rakushev et al. assess that – while suboptimal – the parallel use of Delta and Terminal during the defense of Kyiv was unavoidable due to (a) the lack of standardized hard- and software solutions for processing UAV data, (b) the short timeframe to deploy these systems in the defense of Kyiv, and (c) the difficulty of coordinating the large amounts of volunteer support that was flowing into Kyiv (i.e., volunteer specialist, drone equipment, financial resources etc.).[265]

7 Tooway

Prior to the deployment of Starlink terminals to Ukraine, the European satellite broadband internet service Tooway was the name of the game for many Ukrainian ministries, agencies, and military units.

Tooway was launched in 2007 by utilizing two of Eutelsat's geostationary satellites and ViaSat's Surfbeam technology to bring satellite broadband to Germany, France, Spain, Bulgaria and others.[266] In June 2011, Eutelsat's Tooway satellite service signed a contract with Datagroup to provide broadband to consumers and businesses in

[261] Ibid., p. 58

[262] Ibid., p. 56

[263] Ibid., p. 57

[264] Ibid., p. 58; Michael Sheetz, "SpaceX shipment of Starlink satellite-internet dishes arrives in Ukraine, government official says," *CNBC*, February 28, 2022, https://www.cnbc.com/2022/02/28/ukraine-updates-starlink-satellite-dishes.html

[265] Ракушев et al. "Аналіз використання інформаційно-телекомунікаційної системи "Термінал" в інтересах сил оборони Києва," Modern Information Technologies in the Sphere of Security and Defense, Volume 44, No. 2, September 2022, http://sit.nuou.org.ua/article/view/264158/261332, p. 55

[266] Eutelsat, "Eutelsat and Viasat ready to launch Tooway consumer satellite broadband service in Germany," August 21, 2007, https://www.eutelsat.com/news/compress/en/2007/pdf/PR%202407%20Tooway.pdf or https://archive.ph/wdaWr; Eutelsat, "Eutelsat and Skylogic, in partnership with Viasat, announce new distribution agreements in France, Spain, Bulgaria," September 10, 2007, https://www.eutelsat.com/news/compress/en/2007/pdf/PR%202807%20Tooway.pdf or https://archive.ph/QDcik

Ukraine. [267] Datagroup did not – and still does not – have its own satellites in orbit. Instead, it is the official reseller of Tooway modems that provide access to Eutelsat's Tooway satellite internet broadband service.
Writing for the Kyiv Independent in September 2022, Daryna Antoniuk put the value of Starlink and Tooway into perspective. According to Antoniuk, "one of [Starlinks] main advantages is speed – up to 200 Mbps. The Ukrainian satellite internet provider Datagroup, Starlink's main rival, offers satellite internet for $43 per month, but its speed is significantly lower – 20 Mbps."[268]

The two significant outcomes from the contract with Eutelsat in 2011 were that: (1) Datagroup subsequently became "the only provider of satellite communication in the KA-SAT range in Ukraine," and (2) the agreement specifically outlined that "the ground network uses ViaSat's SurfBeam® 2 technology."[269] What we also know is that Datagroup is the same satellite internet provider that Aerorozvidka cooperated with back in 2015 to deploy its stationary cameras in the Donbas. It is therefore almost certain that Aerorozvidka used Tooway – and highly likely ViaSat's modems – to transmit its camera feeds to the Ukrainian Armed Forces. On the eve of the Russian invasion, ViaSat's SurfBeam2 and SurfBeam 2+ TooWay modems were targeted by a destructive cyberattack (i.e. a wiper and DDoS attack) that bricked thousands of modems in Ukraine (the so called ViaSat hack).[270] The majority – if not all users in Ukraine – were unable to repair their modems themselves and had to physically ship them to ViaSat to be replaced or refurbished. On May 10, 2022, the US, UK, and EU Council attributed the attack to the Russian Federation without naming a specific threat actor.[271]

A threat intel report published by sekoia.io in March 2022 explained that "thanks to [open-source intelligence] investigations, SEKOIA.IO is able to confirm that KA-SAT was used by the armed forces, the security services and the government of Ukraine prior to the Russian invasion on February 24, 2022 […]. The use of Surfbeam2/Tooway modems is not limited to the Ukrainian army. Several public contacts listed on the government portal prozorro.gov.ua mentioned KA-SAT ground stations purchases using Surfbeam2/Tooway modems. Among other things, four important public contracts with the Data-Group Private Joint Stock Company - the only Ukrainian company that can respond to this public tender according prozorro.gov.ua – draw our attention."[272]

While this CSS report is unable to trace the dissemination of ViaSat's Tooway modems in Ukraine, the logic of the Ukrainian military to buy Tooway equipment was one of pure necessity. In November 2019, the National Defense University of Ukraine published a collected volume titled "The Ukrainian Army: Present and Historical Retrospective." In it, Vyacheslav Sergiyovych Shmyhol, senior lecturer at the Department of General Military Disciplines at the Military Institute of Telecommunications and Informatization, explained that back in 2014-15, one of the main problems for ensuring secure communications within the Ukrainian Armed Forces was that most were Soviet-era systems that were either old and inoperable or could not be used because their technical specifications were known to the enemy.[273] Over time, these communication systems were replaced with Western brands, among them the Tooway satellite service – and with it grew the reliance on ViaSat's Surfbeam modems.[274]

In the same publication, Anton Bondarenko, senior researcher in the department for military and patriot education at National Institute of Ukrainian Studies, further explained that "the use of [Eutelsat's] Tooway satellite communication system made it possible to provide efficient, secure, interactive, high-quality Ethernet communication lines with hundreds and even tens of thousands of remote locations and to organize open and secure telephone communications, video conferencing and the

[267] Eutelsat, "Datagroup selects Eutelsat's TooWay satellite service to roll out broadband to consumers and businesses in Ukraine," June 20, 2011, https://www.eutelsat.com/files/contributed/news/press/en/2011/PR%203911%20Ukraine-Eurosat.pdf

[268] Daryna Antoniuk, "How Elon Musk's Starlink satellite internet keeps Ukraine online," *Kyiv Independent*, September 3, 2022, https://kyivindependent.com/how-elon-musks-starlink-satellite-internet-keeps-ukraine-online/ or https://archive.ph/XTzXf

[269] Eutelsat, "Datagroup selects Eutelsat's TooWay satellite service to roll out broadband to consumers and businesses in Ukraine," June 20, 2011, https://www.eutelsat.com/files/contributed/news/press/en/2011/PR%203911%20Ukraine-Eurosat.pdf

[270] Viasat, "KA-SAT Network cyber attack overview," March 30, 2022, https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview; Marc Colaluca & Nick Saunders, "Defending KA-SAT," Defcon 31, September 15, 2023, https://www.youtube.com/watch?v=gI_ICtX3Gm8

[271] Antony Blinken, "Attribution of Russia's Malicious Cyber Activity Against Ukraine," US Department of State, May 10, 2022, https://www.state.gov/attribution-of-russias-malicious-cyber-activity-against-ukraine/; FCDO, "Russia behind cyber-attack with Europe-wide impact an hour before Ukraine invasion," May 10, 2022, https://www.gov.uk/government/news/russia-behind-cyber-attack-with-europe-wide-impact-an-hour-before-ukraine-invasion; EU Council, "Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union," May 10, 2022, https://www.consilium.europa.eu/en/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union/

[272] Sekoia.io, "Surfbeam2 blackout, what happened with KA-SAT?" FLINT, March 7, 2022, https://f.hubspotusercontent10.net/hubfs/7095517/%5BMarketing%5D%20-%20Ebook-analyse/TLP_WHITE_FLINT%202022-015%20-%20Surfbeam2%20blackout%2C%20what%20happened%20with%20KA-SAT.pdf

[273] Шмиголь В.С. "Проблеми забезпечення зв'язку в зоні проведення АТО у 2014–2015," in "НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ОБОРОНИ УКРАЇНИ імені ІВАНА ЧЕРНЯХОВСЬКОГО, "УКРАЇНСЬКЕ ВІЙСЬКО: СУЧАСНІСТЬ ТА ІСТОРИЧНА РЕТРОСПЕКТИВА," Збірник матеріалів Всеукраїнської науково-практичної конференції 29 листопада 2019, https://nuou.org.ua/assets/documents/uv-sir-conference-2019.pdf, p. 49

[274] Ibid.

transmission of documentary messages between all levels of command, even intelligence information from UAVs to the information processing center."[275] According to a 2022 article by aspi.com.ua, Bondarenko fought in the Donbas from 2014-2015 as part of the Aidar battalion – the same battalion that Aerorozvidka cooperated with to test Fantik.[276]

While it is unclear where exactly within the armed forces ViaSat's Tooway modems were used, there are several indicators that its usage was likely more widespread than previously acknowledged. For example, an online resume of a system engineer called Maksim, notes that he worked for the Department of Telecommunications and Satellite Communications within the Armed Forces of Ukraine from November 2012 to December 2017, tasked with – among other things – "setting up satellite communications tooway."[277] In March 2021, the Poltava Regional Territorial Center for Recruitment and Social Support, stated on its website that "the training will take place at the 179th training center of the communications troops. More than 60 reservists will be involved, including 17 people liable for military service from Poltava region. […] During the training, the participants will acquire theoretical and practical skills in working with military communications equipment and facilities. The training topics include establishing and maintaining communication, using modern communications equipment from Harris, Motorola, Tooway, Aselsan, etc."[278]

It is difficult to gouge whether the ViaSat attack on February 24, 2022, had an overall significant impact on the Ukrainian military. What we do know is that at the time, ViaSat's modems were the only equipment that allowed satellite internet access in Ukraine – including for the Ukrainian Armed Forces – and were the only viable mean to transmit large amounts of data while deployed on the battlefield. In fact, Victor Zhora, then deputy chairman and chief digital transformation officer at the State Service of Special Communications and Information Protection in Ukraine, noted that "[the ViaSat hack] had a serious impact on [the] satellite component of communications," but that satellite communications were not the primary method of communications within the armed forces.[279] What Zora left out is that the ViaSat hack did have a massive impact on all the Ukrainian military systems that heavily relied on satellite internet connectivity, and whose advantage on the battlefield was severely stymied when they were forced to switch to radio and landlines. GIS Arta was one of these systems.

7.1 GIS Arta (ГІС АРТА)

The geographic information system (GIS) Arta is a soft- and hardware solution that allows military headquarters and individual artillery units/tanks to rapidly pull together geographic telemetry data from across the vast battlespace to calculate and coordinate artillery firing solutions. Rapid data processing, coupled with a communications infrastructure to instantly share information between units, massively improved the accuracy and speed of Ukraine's artillery units. According to some reports, GIS Arta reduced the reaction times for receiving artillery support from 20 minutes down to one.[280]

GIS Art was created sometime in 2014 by a group of Ukrainian volunteers who initially tried to remain anonymous. In June 2015, Ukrainska Pravda wrote a lengthy story about the group and even visited the GIS Arta office.[281] The GIS Arta team reminded the journalists not to publish any of their surnames and to blur out all their faces in the photos. Strangely, the team did allow the outlet to publish their real surnames: Boris, Vlodymyr, Viktor, Andriy, Yuriy, and Oleksander. The team also revealed that GIS Arta was essentially a volunteer project of three companies: Geo-Soft, Breeze Software, and PrimWay

[275] Бондаренко А.О., "ВІЙСЬКОВА АГРЕСІЯ РФ: ВІЙНА В ГРУЗІЇ 2008 р., АНЕКСІЯ КРИМУ ТА БОЙОВІ ДІЇ НА ДОНБАСІ 2014," in "НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ОБОРОНИ УКРАЇНИ імені ІВАНА ЧЕРНЯХОВСЬКОГО, "УКРАЇНСЬКЕ ВІЙСЬКО: СУЧАСНІСТЬ ТА ІСТОРИЧНА РЕТРОСПЕКТИВА," Збірник матеріалів Всеукраїнської науково-практичної конференції 29 листопада 2019, https://nuou.org.ua/assets/documents/uv-sir-conference-2019.pdf, p. 21

[276] ASPI, "Український спецзагін "Вовкулаки", який воює на фронті на Сході України, потребує допомоги (Фото, Відео), September 15, 2022, https://aspi.com.ua/news/politika/ukrainskiy-speczagin-vovkulaki-yakiy-voyue-na-fronti-na-skhodi-ukraini-potrebue#gsc.tab=0 or https://archive.ph/NDc62

[277] Work.ua, "Максим - Системный инженер," December 21, 2017, https://www.work.ua/ru/resumes/4370694/ or https://archive.ph/TBEA2

[278] Територіальні центри комплектування та соціальної підтримки Полтавської області, "У Полтаві розпочалися збори оперативного резерву першої черги," March 2, 2021, https://tck.pl.ua/u-poltavi-rozpochalysia-zbory-operatyvnoho-rezervu-pershoi-cherhy/ or https://web.archive.org/web/20230403153707/https://tck.pl.ua/u-poltavi-rozpochalysia-zbory-operatyvnoho-rezervu-pershoi-cherhy/

[279] Kim Zetter, "Viasat Hack "Did Not" Have Huge Impact on Ukrainian Military Communications, Official Says," Zero Day, September 26, 2022, https://www.zetter-zeroday.com/viasat-hack-did-not-have-huge-impact/ or https://web.archive.org/web/20240605204931/https://www.zetter-zeroday.com/viasat-hack-did-not-have-huge-impact/

[280] Cedric Pietralunga, "'The Ukrainian army is a MacGyver army': Ukrainian forces use ingenuity against Russian troops," Le Monde, October 28, 2022, https://www.lemonde.fr/en/international/article/2022/10/28/the-ukrainian-army-is-a-macgyver-army-ukrainian-forces-use-ingenuity-against-russian-troops_6002055_4.html

[281] Українська правда, "Інновації для армії. Система для артилеристів ГІС "Арта'," June 2, 2015, https://life.pravda.com.ua/society/2015/06/2/194846 or https://web.archive.org/web/20240608083019/https://life.pravda.com.ua/society/2015/06/2/194846

Ukraine.[282] It is unknown when exactly the GIS Arta team revealed their identities publicly. Safe to say, in July 2016, Ukraine's New Voice media outlet wrote that Boris Kostenko was the founder of Primway Ukraine. Viktor Smetanyuk was the founder of Breeze Soft. And Vladimir Popov was the head of Geo-Soft.[283]

Figure 46-48: (left) Bricked ViaSat Tooway modem; (center) GIS Arta's satellite suite; (right) GIS Arta & ViaSat modem use in Ukraine

Source: (left) Marc Colaluca & Nick Saunders, "Defending KA-SAT," Defcon 31, September 15, 2023, https://www.youtube.com/watch?v=gl_ICtX3Gm8, time stamp: 18:21-19:46; (center) ГІС Арта, "З усім цим ГІС "Арта" вже подружилася," Facebook, March 20, 2015, https://www.facebook.com/gis.arta/photos/1566838880222834 or https://archive.ph/fdP2T ; (right) ГІС Арта, "Привіт камради..Ми знову у полях.." Facebook, November 19, 2015, https://www.facebook.com/gis.arta/posts/1640862512820470 or https://archive.ph/NpMVv

Some Western reports have claimed that GIS Arta was developed by Yaroslav Sherstyuk.[284] Sherstyuk is well-known in the Ukrainian military community for having developed ArtOS, MilChat, MyGun and a handful of other mobile artillery and communications applications that are still being used by the Ukrainian Armed Forces. Notably, in 2016, CrowdStrike revealed that between late-2014 to 2016, Russian military intelligence (APT28/Fancy Bear) disseminated a malware infected version of Sherstyuk's Поправки-Д30 (Engl. transl.: Correction-D30) mobile application on Ukrainian military fora.[285]

As far as Ukrainian open source is concerned, Yaroslav Sherstsyuk was not involved in the development of GIS Arta, and neither was his then employer UkropSoft. The development of ArtOS and GIS Arta were entirely separate efforts.[286] That being said, although ArtOS can feed data and information into Delta, the system will not be covered in this report, because the last news item on the ArtOS website is from eight years ago.[287] As of this writing, Sherstyuk is a project manager at Telekart-Prylad, the same company that developed the ACS Prostir system (see the section on Dzvin).[288]

With the start of the Russian invasion in 2022, many Western media outlets started to cover the success story of GIS Arta. Dubbed the "Uber for Artillery," much of the reporting was focused on GIS Arta's efficiency on the battlefield, with very few covering its dependence on ViaSat.

Speaking to Ukrainska Pravda in June 2015, the group explained how the GIS Arta system was set up. The military headquarters or situational center is in possession of a laptop with the GIS Arta software. The laptop is connected to a small black box. Boris Kostenko explained that "this is where the satellite, American Harris or Motorola (walkie-talkies) are connected, and here are the broadband data channels. Everything is encrypted, the communication is absolutely secure."[289] While the team jokingly stated that "the satellite is foreign, commercial. You can write that it is Chinese,"[290] GIS Arta was entirely reliant on

[282] Ibid.

[283] Мыкола Олиярнык, "Наука побеждать," New Voice, July 15, 1016, https://nv.ua/magazine/journal/n25s_15072016/nauka-pobezhdat-20005809.html or https://archive.ph/8ZZhO

[284] David Zikusoka, "How Ukraine's "Uber for Artillery" is Leading the Software War Against Russia," New America, n.d., https://www.newamerica.org/future-frontlines/blogs/how-ukraines-uber-for-artillery-is-leading-the-software-war-against-russia/; Mark Bruno, ""Uber For Artillery" – What is Ukraine's GIS Arta System?" August 24, 2022, https://themoloch.com/conflict/uber-for-artillery-what-is-ukraines-gis-arta-system/; Philippe Langloit, "L'exemple de Gis Art Artillery. L'innovation par le bas, vainqueur en Ukraine?" aerion24, June 20, 2022, https://www.areion24.news/2022/06/20/lexemple-de-gis-art-artillery-linnovation-par-le-bas-vainqueur-en-ukraine/

[285] CrowdStrike, "Use of Fancy Bear Android Malware in tracking of Ukrainian field artillery units," 2016, https://www.crowdstrike.com/wp-content/brochures/FancyBearTracksUkrainianArtillery.pdf

[286] Українська правда, "Артиллерийская математика. История разработчика Ярослава Шерстюка," November 8, 2015, https://life.pravda.com.ua/society/2015/11/8/202830/; ArtOS website, May 18, 2024, https://web.archive.org/web/20240606113354/https://artos.tech/; GIS Arta website, May 18, 2024, https://web.archive.org/web/20240518155738/https://gisarta.org/en/#about

[287] ArtOS, "ArtOS complex: purpose, advantages and prospects," October 29, 2017, https://artos.tech/uk/kompleks-artos-pryznachennia-perevahy-ta-perspektyvy or https://web.archive.org/web/20240606125150/https://artos.tech/uk/kompleks-artos-pryznachennia-perevahy-ta-perspektyvy

[288] Linkedin, Yaroslav Sherstyuk's Linkedin profile, https://www.linkedin.com/in/ярослав-шерстюк-a5015bb3/

[289] Українська правда, "Інновації для армії. Система для артилеристів ГІС 'Арта'," June 2, 2015, https://life.pravda.com.ua/society/2015/06/2/194846 or https://web.archive.org/web/20240605204949/https://life.pravda.com.ua/society/2015/06/2/194846

[290] Ibid.

Eutelsat's Tooway service for its satellite broadband connection.

In May 2019, 24tv.ua published an op-ed by the Ukrainian NGO Come Back Alive (more on them in the next section) talking about GIS Arta's functionalities and costs. The op-ed explained that, "so, on their own enthusiasm, working nights and in all their free time, the guys created a program that had an important advantage over similar ones. The program runs on secure laptops, creating a network that is not hierarchical. The program has a map and functionality for mapping targets, creating databases, managing combat, and more. At the same time, each Arta GIS laptop is an independent server that has its own access to satellite communications, can work both independently (offline, regardless of the availability of the Internet) and online - to exchange data via secure communication."[291] The article goes on to note that "the number of laptops at the front is now about 200, almost all units are provided with them, and the total cost of satellite communications has reached UAH 1 million per year (~39.000 USD at the time)."[292] In July 2022, the developers of GIS Arta explained to Watson.ch that "Starlink is one of our channels. It has a big advantage compared to others - flexibility. Before that, we used Viasat. But there were critical problems there [i.e. the ViaSat hack] and we stopped using it."[293]

For GIS Arta, satellite communications were the dominant vector to promptly relay data and contextual information to multiple artillery units deployed in the field. While, depending on the relative distance between the artillery units and ongoing Russian jamming efforts, some information could be conveyed via radio, the ViaSat hack likely had a detrimental effect on the use of GIS Arta on the battlefield. The hack highly likely forced artillery units to switch to pure radio communications, which in turn likely impacted the data throughput, the ability to flexibility coordinate artillery fires, and the time for units to receive artillery support.
As of this writing, GIS Arta has not publicly spoken about how they operated during the time between the ViaSat hack and the arrival of Starlink terminals in Ukraine.

7.2 Come Back Alive

In May 2015, GIS Arta started to cooperate with the Ukrainian non-profit charity foundation Come Back Alive.[294] Speaking to fakty.com.ua in 2021, GIS Arta's Borys Kostenko explained that "until the middle of spring 2015, we bought kits for the Armed Forces at our own expense. But the need is much greater, so in May 2015, we started cooperating with the Come Back Alive Foundation. The foundation buys the equipment, i.e. hardware, [with] charitable funds, passes it to us, we fill it with [the software], and hand them over to the Come Back Alive Foundation under the acts of delivery. We do the [software] and all the installation work [with] our own money."[295]

Come Back Alive was founded by Kyiv-based IT specialist Vitaliy Deynega back in 2014 with a focus on raising money to purchase body armor for the Ukrainian Armed Forces. Deynega wrote 'come back alive' on each vest he sent to the front lines, hence the name of the foundation. Over the years, the Ukrainian government actively promoted Come Back Alive to the degree that it eventually became the first charity organization in Ukraine to purchase and import military and dual-use goods, including the Bayraktar TB2 UAV drone system.[296] The Come Back Alive website also notes that, "our instructors have trained over 10,000 highly skilled military specialists, including EOD professionals, snipers, drone operators, and infantry weaponry experts. They also provide first-aid training and set up medical training complexes within the Armed Forces. Additionally, they assist with confidential missions, details of which we will disclose after Ukraine's victory."[297]

With the deployment of Russian military forces along the border in preparation for the 2022 invasion, the prominence of Come Back Alive exploded, making it by far the largest and most well-known charity foundation assisting the Ukrainian Armed Forces. As of April 2024, the fund has raised 341 million USD since its founding a decade ago.[298]

But with international fame also came blowbacks. Two days after the Russian invasion, US-headquartered

[291] Повернись живим, "Група ентузіастів-програмістів створила програму, яка допомагає українським військовим," 24tv.ua, May 15, 2019, https://24tv.ua/ru/grupa_entuziastiv_programistiv_stvorila_programu_yaka_dopomagaye_ukrayinskim_viyskovim_n1316779 or https://archive.ph/tO6uJ

[292] Ibid.

[293] Daniel Schurter, "This is how Ukraine's secret "superweapon" works – and what its developers say," Watson.ch, July 24, 2022, https://www.watson.ch/digital/analyse/588967715-gis-arta-so-funktioniert-die-heimliche-superwaffe-der-ukraine

[294] Юлія Захарченко, "Це коштуватиме дорого Росії: військовий волонтер про можливу агресію проти України," fakty, December 5, 2021, https://fakty.com.ua/ua/ukraine/suspilstvo/20211205-cze-koshtuvatyme-dorogo-dlya-rosiyi-vijskovyj-volonter-pro-mozhlyvu-agresiyu-proty-ukrayiny/ or https://archive.ph/ezd5a

[295] Ibid.

[296] Come Back Alive, "About the Foundation," n.d., https://savelife.in.ua/en/about-foundation-en/ or https://archive.ph/Mzgvj

[297] Ibid.

[298] Ibid.

crowdsourcing start-up Patreon, suspended the foundation's account for violating its policies. Prior to the ban, Come Back Alive had 936 patrons that gave the foundation around 19.000 USD per month.[299] With the invasion, the number skyrocketed to almost 15.000 patrons generating over 300.000 USD.[300] In a blog post Patreon explained that it does not allow its platform to "be used for funding weapons or military activity."[301] All the donations in Come Back Alive's Patron account were refunded to the individual contributors and the fund's Patreon account was shut down.

Figure 49: Come Back Alive's Cyber Fundraiser

Source: Come Back Alive & Portmone fundraising website, July 12, 2024, https://cyberdef.savelife.in.ua/en/

On February 20, 2023, Come Back Alive in cooperation with the General Staff of the Armed Forces launched a 1.2 million USD fundraiser to assist in "building infrastructure" and purchasing "system, network, and other equipment for the arrangement of a data center" for the cyber forces of the Armed Forces of Ukraine.[302] As Andriy Rymaruk, head of the military department of Come Back Alive explained, "we actually raise money for cyber offensive. It will burn even in the most rotten heart of the occupying country."[303] In similar vein, Come Back Alive noted that, while it will not disclose the entire list of all purchases, "every hryvnia spent will work to complicate the logistics and control of enemy troops, as well as to identify the locations of russian occupiers and their further effective destruction by other units of the Armed Forces."[304]
On February 21, 2023 – one day after launching the cyber forces' fundraiser – Vitaliy Deynega was appointed Deputy Minister of Defense for Digital Development, Digital Transformations, and Digitalization.[305]

Because of the larger than usual public interest in this particular fundraising effort, Come Back Alive published a follow-up article explaining that, the "technical means will provide intelligence information that the Armed Forces will use when planning actions on a real battlefield [possibly laptops and tablets to run Delta and other applications on]. The data center will also be used to search for enemy vulnerabilities and critical elements of their infrastructure, including cyber infrastructure."[306] Come Back Alive publicly disclosed that they bought "a 72 kW generator, two uninterruptible power supplies, and a backup power panel," for the cyber forces.[307] The cyber forces fundraiser was approved by the General Staff of the Armed Forces and was publicly endorsed by the Communications and Cyber Security Forces Command of Ukraine.[308]

Yet despite the available open-source information it is still unclear which exact unit was the beneficiary of the cyber forces' fundraiser. As of this writing, the law on creating the 'Cyber Forces of the Armed Forces of Ukraine' is still being drafted.[309] Speaking to ain.ua in December 2023, Vladyslav Hryzev – head of the recruitment agency Lobby X – offered one potential explanation by noting that, "the Cyber Force de facto exists […]. Today, they are actually a department. I can't tell you in which structure, but the Cyber Force exists and is working - with our help, they

[299] Mikael Thalen, "No, you can't use Patreon to buy missiles for Ukraine (updated)," *Daily Dot*, February 24, 2022, https://www.dailydot.com/debug/patreon-missiles-ukraine/

[300] Ibid.; Jordan Novet, "Patreon suspends donation page for nonprofit giving body armor to Ukrainian army," *CNBC*, February 24, 2022, https://www.cnbc.com/2022/02/24/patreon-suspends-come-back-alive-page-for-ukrainian-army-donations.html

[301] Patreon, "On the removal of Come Back Alive," February 25, 2022, https://news.patreon.com/articles/on-the-removal-of-come-back-alive

[302] Come Back Alive, Cyber Fundraiser, n.d., https://cyberdef.savelife.in.ua/en/#who or https://archive.ph/5y0om

[303] Maksym Lymanskyi, "Come Back Alive announces fundraising for cyber offensive," Come Back Alive, February 20, 2023, https://savelife.in.ua/en/materials/news-en/come-back-alive-announces-fundraising-fo-en/ or https://archive.ph/7Loh8

[304] Ibid.

[305] ЄЛИЗАВЕТА ДРАБКІНА, "Кабмін призначив ще двох заступників Резнікова," *РБК-Україна*, February 21, 2023, https://www.rbc.ua/rus/news/kabmin-priznachiv-shche-dvoh-zastupnikiv-1676989710.html or https://archive.ph/ehhjZ

[306] Maksym Lymanskyi, "The cyber fundraiser Come Back Alive has raised over a million: New details of the project," Come Back Alive, 23 February 2023, https://savelife.in.ua/en/materials/news-en/the-cyber-fundraiser-come-back-alive-has-en/ or https://archive.ph/YhNeK

[307] Come Back Alive, Cyber Fundraiser, n.d., https://cyberdef.savelife.in.ua/en/#who or https://archive.ph/5y0om

[308] Командування Військ зв'язку та кібербезпеки Збройних Сил України,"Підтримуємо побратимів!" *Facebook*, February 23, 2023, https://www.facebook.com/signalcybersecutiry-command/posts/pfbid04eKSNEfjr9FZYhUabtJWotS-NAmG4f3qw39kAXLGsXDVVNqtLFBCTrWjWPbdXtjb2l or https://archive.ph/cp43n; Come Back Alive, Cyber Fundraiser, n.d., https://cyberdef.savelife.in.ua/en/#who or https://archive.ph/5y0om

[309] Софія Єлагіна," Законопроєкт про Кіберсили ЗСУ вже обговорюють у МО та Силах оборони. Ми дізнались більше про майбутній рід військ," *ain.ua*, May 8, 2024, https://ain.ua/2024/05/08/cyberforce/ or https://archive.ph/cqqBe

have staffed the specialists, we are satisfied with the level of specialists, and we are constantly in contact with their command. I also know that the Cyber Force is satisfied with its results. Of course, they are not very public and do not go into PR, but rather focus on the result. Let me give you an example: do you remember the recent hacking of the Russian tax system by the Main Intelligence Directorate? As far as I know, the GUR itself does not have a separate unit that deals with cyber events. So we have the right to suspect that someone else did it."[310]
Notably, this was not the first time Come Back Alive provided funds to the Ukrainian cyber forces. According to the foundation itself, it gave 8.7 million UAH (~220.000 USD) to the cyber forces in 2022.[311]

8 Further Thoughts

At its core, Delta is a platform that was born out of military necessity to (a) integrate from the bottom up a variety of different information sources and data formats, and (b) share said data and information as widely and as easily accessible as possible. This inherent openness necessitates specific digital infrastructure demands: Delta's deployment in the public cloud, intelligence cells and situational centers that collect, check, and feed data into the platform, as well as the portability demand to access Delta from anywhere on the battlefield. On top of these requirements, there is the need to secure the platform, physical devices, and Delta users from malicious intrusions and captivity. Underpinning all of this is the training to familiarize users on how to deploy, utilize, and securely access Delta and its parts.

The resulting ecosystem has largely flourished due to mutual buy-ins. Ukrainian volunteers have more or less naturally cooperated with each other to provide IT solutions and capabilities to the Ukrainian Armed Forces – some of which the Ukrainian military did not even know it needed. What is important to stress in this context is that these groups did not replace the Ukrainian Armed Forces. Taras Chmut, the current head of Come Back Alive, put it most elegantly when he said in 2022 that "the volunteer movement is not substituting the government, it's a helping hand."[312] This is both true in kinetic space, as it is in cyber and the digital realm.
The Ukrainian Armed Forces on the other hand had to learn how to deal and cooperate with a variety of volunteer groups that arrived with particularly strong convictions, existing relationships, and expectations. For its part, Aerorozvidka had probably the strongest buy-in from all other volunteer groups due to (a) its direct relationship to several NATO member states via the NATO-Ukraine C4 Trust Fund, and (b) its political endorsement at home – including by then President Petro Poroshenko. Aerorozvidka's innovations on the battlefield – first via drones, then with stationary cameras – provided a stable foundation to better understand the need of the Ukrainian Armed Forces and eventually become – with unit A2724 – the center for technical innovation within the Ukrainian military. Steady government and military buy-ins (political & technical support), continuous accumulation of knowledge, talent, and nurturing relationships (constant evolution), combined with operational deployments on the kinetic battlefield (practice), are the trifecta that have made Aerorozvidka so successful.

Recommendation: Western militaries and policymakers must think about how they can mobilize their own expat communities abroad. Particularly those that work in the areas of IT, journalism, marketing, and fundraising activities. Western militaries must also think about how to create ad-hoc relationships across all their domestic talent pools – including veterans, pensioners, university/high school students, and walk-in volunteers. Depending on the conflict scenario at hand, mobilizing the global IT community might also be a distinct possibility which will necessitate active engagement and political narrative shaping.

Delta export and replication

When it comes to Delta specifically, it is unclear whether the success of the platform can be replicated outside of Ukraine. Part of the problem is Delta's dependence on the goodwill of non-Ukrainian private sector companies. For example, Telegram could choose to ban the eEnemy and Stop Russian War bots. Google and Apple could kick

[310] Олександр Стрельников, "«Без людей на «передку» не обійдешся, треба всім це усвідомити». Владислав Грезєв з Lobby X — про рекрутинг в ЗСУ й проблеми армії," *ain.ua*, December 20, 2023, https://ain.ua/2023/12/20/vladyslav-grezyev-z-lobby-x-pro-rekrutyng-v-zsu-j-problemy-armiyi/ or https://archive.ph/47Nwn; For a critical analysis on GURMO's activities in cyberspace see: Stefan Soesanto, "Smoke, Mirrors, and Self-Attribution: Ukraine's Military Intelligence Service in Cyberspace," *RealClearDefense*, March 2, 2024, https://www.realcleardefense.com/articles/2024/03/02/smoke_mirrors_and_self-attribution_ukraines_military_intelligence_service_in_cyberspace_1015598.html

[311] Maksym Lymanskyi, "The cyber fundraiser Come Back Alive has raised over a million: New details of the project," Come Back Alive, 23 February 2023, https://savelife.in.ua/en/materials/news-en/the-cyber-fundraiser-come-back-alive-has-en/ or https://archive.ph/YhNeK

[312] Illia Ponomarenko, "Head of Come Back Alive foundation: 'If you want to help Ukraine's military, buy equipment," The Kyiv Independent, September 8, 2022, https://kyivindependent.com/taras-chmut-if-you-want-to-help-ukraines-military-buy-communication-equipment/ or https://web.archive.org/web/20240614093407/https://kyivindependent.com/taras-chmut-if-you-want-to-help-ukraines-military-buy-communication-equipment/

Bachu, ePPO, and all other Ukrainian military mobile applications off its app stores. And SpaceX could disable Starlink access if the risks of operating in Ukraine outweighs its contractual obligations to Western governments and Ukrainian customers. Without Starlink, Delta loses its mobility advantage. And without Telegram, Google, and Apple it loses large parts of its crowdsourced intelligence stream. There are very few – if any – services and platforms that are able to fill these major capability gaps.

For the time being, if Delta were to be exported to any other country, so would also the demand to use Starlink terminals, host military apps on Google and Apple app stores, and maybe even the creation of channels on Telegram. Some countries might be able to leverage domestic alternatives to these services, but it is doubtful whether they can be implemented as broadly and easily as we are witnessing in Ukraine.
That being said, in the absence of clear and steadfast policy guidelines as to when Starlink can be used in a military context and what kind of mobile applications for warfare are allowed to be hosted on Google Play and Apple store, the appeal to rely on US-headquartered companies – and with it pulling US foreign policy interests into a conflict – is likely too attractive for foreign governments to resist. Thus, if Delta were to be exported, we will likely see Washington struggle to find a coherent foreign policy narrative for each case, and Western companies will likely have to decide themselves which belligerents to tacitly support, and which ones to actively deny service. Some of these decisions will highly likely be driven by economic interests and sunk costs – as witnessed by the behaviour of Western companies still conducting business in Russia, while others will make decisions for the sake of political posturing, company branding, and maybe a moral compass which might be prone to go haywire in highly emotional and partisan conflict scenarios.

Dubai-based Telegram has struggled with some of these questions back in 2022 when it wanted to restrict numerous Telegram channels in Russia and Ukraine, because they were used for military propaganda. In the end, Telegram took the neutral approach and opposed restrictions, as users wanted the freedom to access information, even when that information was biased. While this was a prudent choice, it is also leading to constant bickering and accusations. For example, on April 28, Telegram blocked the eEnemy bot and Ukraine's military intelligence (GURMO) subsequently accused the company of violating its own rules and public statements. One day later, Telegram restored access to eEnemy, explaining that it was "temporarily disabled due to a false positive."[313] As of this writing, there are ongoing political discussions in Ukraine on whether to ban or regulate Telegram in some way shape or form.[314]

The export of Delta will likely also entail Ukrainian military advisors teaching foreign military personnel on how to use Delta, Starlink, and Ukrainian-made drones efficiently. It seems likely that Kyiv will utilize the export of Delta to build relationships and military ties across the globe to continue its fight against Russian – and possibly Chinese – geopolitical influence abroad. The massive build-up of Ukraine's miltech sector will highly likely underpin Kyiv's global counter-Russia efforts in the long run, with Delta serving as the integrator platform for numerous current and future Ukrainian miltech products. How Ukraine's miltech exports will be viewed in Washington and the European capitals is currently anyone's best guess.

Western militaries would do well to think about what components of Delta they are interested and willing to replicate. Probably the most attractive element is Delta's crowdsourced intelligence via eEnemy, Stop Russian War, and Bachu. From a technical point of view, it is very easy to design and create these applications and bots. The major challenge is their broad adoption within society – which is tied at the hip to (a) citizens trusting their military and intelligence services, and (b) the state of a country's digitalization.

The crowdsourcing element is particularly interesting, because it likely fosters within society a sort of buy-in and sense of actively helping the war effort. This psychological effect stands on par with the Ukrainian government's cooperation with expats abroad and volunteers at home to incorporate a flourishing self-organized ecosystem that actively tries to support the war effort through fundraising, buying military equipment, and developing applications and drones. The incorporation of civilians in modern warfare – whether it is in the digital space or outside of it – is likely a crucial component to sustain and increase the effectiveness of non-expeditionary military operations.

Recommendation: Of particular value for the replication debate would be a legal analysis on how and whether the

[313] Daryna Antoniuk, "Telegram blocks, then unblocks, chatbots used by Ukraine's intelligence services," TheRecord, April 29, 2024, https://therecord.media/telegram-blocks-chatbots-used-by-ukraine

[314] Pavlo Bashynskyi, "Telegram poses a number of threats to Ukraine's security – Yusov," *Unn.ua*, February 14, 2024, https://unn.ua/en/news/telegram-poses-a-number-of-threats-to-ukraines-security-yusov; NV, "Ukraine's top spy Budanov advocates for Telegram regulation, not mere influence or pressure," April 22, 2024, https://english.nv.ua/nation/telegram-regulation-needed-not-influence-or-pressure-says-ukraine-s-spy-chief-budanov-50412143.html

Ukrainian government's implementation of eEnemy – i.e. interfacing with both the official Ukrainian e-government app (Diia) and the country's premier military situational awareness platform (Delta) – is in line with international humanitarian law.

That being said, different countries will likely run into different hurdles for replicating Delta's crowdsourcing applications. Some will face severe privacy issues and questions of IHL, while others will meet political resistance. On the other hand, Ukraine has proven that its implementations, whether they are websites displaying videos of Russian prisoners of war, misusing Starlink for military operations, and enabling civilians to transmit targeting data directly to the military, faced little to no scrutiny from Western policymakers, academics, think tankers, and armchair generals. Maybe we have entered a period of history in which the fear of a future global armed conflict allows militaries to replicate what they otherwise would have been denied inventing themselves.

Destructive cyberattacks

On the Russian side there have been some efforts to replicate Ukrainian miltech products – including Kropyva and ePPO. As of this writing, these have not been as successful nor are they as widely disseminated as the Ukrainian originals. There are currently no known Russian efforts to replicate Delta. While Russian cyber campaigns are continuously targeting various components that make up the Delta ecosystem, the most fruitful measures so far have been the selective jamming of Starlink (i.e. Russian electronic warfare measures).[315] Given Russia's success in bricking thousands of ViaSat's Tooway Surfbeam 2 modems in the beginning of the war, a future destructive cyberattack against Starlink is a distinct possibility, particularly if Russia's General Staff comes to the conclusion that jamming efforts are insufficient. For the time being though, Russian adoption of Starlink terminals on the frontlines seems to be the preferred option to take advantage of Starlink rather expediting efforts to take it down. At the same time, Russian efforts to probe Starlink's network, terminals, and connected Ukrainian military devices are ongoing.[316]

It is unknown whether Russian intelligence was already aware of Delta's potential to shape Ukraine's way of digital warfighting back in 2016-2020. It would be logical to assume that Delta's development within the NATO-Ukraine C4 Trust Fund and President Poroshenko's direct financing of Delta did not escape their knowledge. If this assumption is correct, then Russian intelligence likely shifted more and more resources into efforts to breach Delta once the platform was deployed on the battlefield. With each device and application that was added to feed data into Delta, the attack surface expanded – and with it likely also the resources devoted by Russian intelligence to breach them.

It is unclear whether Russian intelligence is aware of the physical location of the servers on which Delta is hosted. It seems unlikely that those servers are not located in any of the frontline oblasts. Except for maybe in hardened military infrastructure or – if the Ukrainian military is really pushing it – in residential areas to disguise it. Strategically it would probably make sense to locate them in the eastern part of Ukraine close to the Polish border to prevent electricity outages and guarantee political fallout if it were targeted by missile strikes and sabotage attempts. If Russian military and intelligence is unable to physically touch the servers, then the cyber component is the only vector to take out the platform. As Aerorozvidka NGO is steadily hardening the accounts of Delta users, the most likely expectation is that current Russian efforts are focused on geolocating Delta users on the battlefield via compromised applications, social media use, or even targeting their families and friends to (a) intercept a Delta user's communications in the electromagnetic spectrum or (b) capture the user and recover their devices to gain access to Delta. Thus, rather than a stand-off remote capability to breach and compromise a system, the bulk of Russian cyber capabilities are likely transforming to function as part and parcel of ongoing tactical operations on the battlefield with cyber operators embedded in frontline units.

To some degree this could explain why we have not witnessed an onslaught of destructive Russian cyber campaigns against Ukrainian critical infrastructure over the past year.

Recommendation: Cyber scholars and think tankers would do well to focus their research on electronic warfare and the intersection of cyber and EW – also known as CEMA (cyber electromagnetic activity). Rather than just

[315] Paul Mozur & Adam Satariano, "Russia, in New Push, Increasingly Disrupts Ukraine's Starlink Service," *The New York Times*, May 25, 2024, https://www.nytimes.com/2024/05/24/technology/ukraine-russia-starlink.html; Yevhen Kizilov, "Ukrainian military's Starlink terminals went down at beginning of Russian offensive in Kharkiv Oblast," *Ukrainska Pravda*, May 17, 2024, https://www.pravda.com.ua/eng/news/2024/05/17/7456272/

[316] Thomas Grove et al, "The Black Market That Delivers Elon Musk's Starlink to U.S. Foes," *The Wall Street Journal*, April 9, 2024, https://www.wsj.com/business/telecom/starlink-musk-ukraine-russia-sudan-satellite-communications-technology-f4fc79d9?st=kgdepwl5vec2cdb&reflink=article_email_share; Daryna Antoniuk, "Ukraine says it thwarted attempt to breach military tablets," TheRecord, August 8, 2023, https://therecord.media/ukraine-military-tablets-sandworm-hacking-attempt

viewing cyber as an isolated stand-off capability, the reality on the Ukrainian battlefield is moving toward overlapping mission requirements and tactical integration. Russian cyber operators working side-by-side with special operations forces and electronic warfare officers is where the innovation of cyber in war is at.

(For a primer on the CEMA topic see: Stefan Soesanto, "A Digital Army: Synergies on the Battlefield and the Development of Cyber-Electromagnetic Activities (CEMA)," September 2021, Cyber Defense Report, Center for Security Studies, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2021-08-Creating-Synergies-on-the-Battlefield-CEMA.pdf)

Hosting Delta on cloud servers abroad

Moving Delta onto cloud servers outside Ukraine is potentially a double-edged sword whose cost-benefit calculations are not as straightforward as the Ukrainian government portrays them to be. Rather than better protecting Delta from cyber- and missile attacks, a hosting server abroad will likely become a massive target for Russian sabotage and cyber warfare efforts. Thus, rather than protecting Delta, it will paint a big red target onto the cloud provider, the provider's other customers, and the government on whose territory the servers are physically located in, which in turn will likely lead to further escalation – if not co-belligerency. For the Ukrainian government, it is equally important to ascertain whether it can actually trust the cloud provider and the foreign government to secure the server farm from insider threats, physical sabotage campaigns, regulators, and potential lawsuits. Any government and cloud provider that is going to host Delta amidst the ongoing international armed conflict in Ukraine will operate in a scenario of political unknowns, legal uncertainty, and exacerbated security challenges.

That beings said, Western governments could think about turning the equation on its head, by allowing foreign government to host their digital platforms on servers in Western countries prior to the outbreak of conflict. One such scenario could entail Taiwan.

Recommendation: Western governments would do well to figure out what third-country software products used for war can – or should not be allowed to – be hosted on cloud servers located on their territory. A comprehensive legal analysis might be necessary to identify classification criteria, regulatory loopholes, and company transparency requirements.

On July 11, 2024, Aerorozvidka celebrated its 10th anniversary with a series of talks published on Youtube (see: https://www.youtube.com/watch?v=9Jxf2w0N9fg).

List of Acronyms

2FA	Two Factor Authentication
ACS	Automatic Control System
ACT	Allied Command Transformation
AFCEA	Armed Forces Communications & Electronics Association
AFU	Armed Forces of Ukraine
APT	Advanced Persistent Threat
AWS	Amazon Web Service
C3	Command, Control, and Communications
C4	Command, Control, Communications, and Computer
C4I	Command, Control, Communications, Computers, and Intelligence
CWIX	Coalition Warrior Interoperability eXploration, eXperimentation, eXamination eXercise
DDoS	Distributed Denial of Service
DJI	Dà Jiāng Chuàngxīn
DSHV	Ukrainian Air Assault Forces
EA	Enterprise Architecture
EOD	Explosive Ordnance Disposal
GIS	Geographic Information System
GPS	Global Positioning System
GRU	Main Directorate of the General Staff of the Armed Forces of the Russian Federation
GUR/ GURMO	Main Directorate of Intelligence of the Ministry of Defence of Ukraine
HRW	Human Rights Watch
IP	Internet Protocol
ISTAR	Intelligence, surveillance, target acquisition, and reconnaissance
JDSS	Joint Dismounted Soldier System
JFO	Joint Forces Operation
LLM	Large Language Models
NGO	Non-governmental Organization
NV	New Voice
POW	Prisoner of War
SBU	Security Service of Ukraine
SEDO-M	Secure Electronic Documents Management System
SESU	State Emergency Service of Ukraine
SSSCIP	State Service for Special Communications and Information Protection of Ukraine
SSO	Ukrainian Special Operations Forces
STANAG	NATO Standardization Agreement
TIDE	Think-Tank for Information Decision and Execution Superiority
TTPs	Tactics, Techniques, and Procedures
UAH	Ukrainian hryvnia
UAV	Unmanned Aerial Vehicle
VPN	Virtual Private Network

About the Author

Stefan Soesanto is a Senior Researcher at the Center for Security Studies (CSS) at ETH Zurich. He leads the Cyberdefense Project and is the Co-Team Head of the Risk and Resilience Team.

Prior to joining CSS in 2019, he was the Cybersecurity & Defense Fellow at the European Council on Foreign Relations (ECFR) and a non-resident James A. Kelly Fellow at Pacific Forum CSIS. Stefan also served as a Research Assistant at RAND's Brussels office, co-authoring reports for the European Parliament Committee on Civil Liberties, Justice and Home Affairs (LIBE), the European Network Information Security Agency (ENISA), and Dutch Ministry of Security and Justice.

Stefan holds an MA from Yonsei University (South Korea) with a focus on security policies, and international law, and a BA from the Ruhr-University Bochum (Germany) in political science and Japanese.

CSS
ETH Zürich

The **Center for Security Studies (CSS)** at ETH Zürich is a center of competence for Swiss and international security policy. It offers security policy expertise in research, teaching and consulting. The CSS promotes understanding of security policy challenges as a contribution to a more peaceful world. Its work is independent, practice-relevant, and based on a sound academic footing.